StoreFront 3.11

May 22, 2017

ストアに表示するリソースの管理

NetScaler Gatewayを介したストアへのリモートアクセスの管理

Citrix Onlineアプリケーションをストアに統合する

Configure two StoreFront stores to share a common subscription datastore

上級ストア設定

Manage a Citrix Receiver for a Web site

Citrix Receiver for Webサイトの作成

Configure Citrix Receiver for Web sites

統合Citrix Receiverエクスペリエンスのサポート

おすすめのアプリケーションの作成および管理

ワークスペースコントロールの構成

Citrix Receiver for HTML5のブラウザータブ使用の構成

通信のタイムアウト期間および再試行回数の構成

Configure user access

Configure high availability for stores

Integrate with NetScaler and NetScaler Gateway

NetScaler Gateway接続の追加

NetScaler Gatewayアプライアンスのインポート

NetScaler Gateway接続設定の構成

NetScalerによる負荷分散

Configure two URLs for the same NetScaler Gateway

Configure NetScaler and StoreFront for Delegated Forms Authentication (DFA)

ビーコンポイントの構成

Advanced configurations

Configure Desktop Appliance sites

Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally

Configure Resource Filtering

Configure using configuration files

Configure StoreFront using the configuration files

構成ファイルを使ったCitrix Receiver for Webサイトの構成

Secure your StoreFront deployment

StoreFront SDK

Troubleshoot StoreFront

Citrix SCOM Management Pack for StoreFront

Citrix SCOM Management Pack for License Server

About StoreFront

May 30, 2017

StoreFront manages the delivery of desktops and applications from XenApp and XenDesktop servers, and XenMobile servers in the data center to user devices. StoreFront enumerates and aggregates available desktops and applications into stores. Users access StoreFront stores through Citrix Receiver directly or by browsing to a Citrix Receiver for Web or Desktop Appliance site. Users can also access StoreFront using thin clients and other end-user-compatible devices through a XenApp Services site.

StoreFront keeps a record of each user's applications and automatically updates their devices. Users have a consistent experience as they roam between their smartphones, tablets, laptops, and desktop computers. StoreFront is an integral component of XenApp 7.x and XenDesktop 7.x but can be used with several versions of XenApp and XenDesktop.

StoreFront 3.11 includes a number of fixed and known issues.

Fixed issues

May 22, 2017

The following issues have been fixed since version 3.9:

- If the Citrix SCOM Management Pack Agent service is installed on the StoreFront server, StoreFront cannot upgrade.

  [#DNA-34792]

- On upgrade, StoreFront forgets the default IIS website setting. This issue applies to upgrades from versions 3.5, 3.6, 3.7, or 3.8.

  [#DNA-22721]

- StoreFront does not upgrade with a large (over 2 GB) subscription database.

  [#DNA-27194]

- Cannot log on to Citrix Receiver for Web site using domain pass-through in a shared authorization service environment. If you have multiple stores sharing an authorization service and then create a new, dedicated authentication service for one of the stores, it is not possible to log on to the Citrix Receiver for Web site while using domain pass-through.

  [#DNA-34238]

- Attempts to launch a session might fail with the following error message:

  "The ICA file contains an invalid unsigned parameter."

  Before you upgrade or replace the new ADMX file, set the ICA file signing related policy "Enable ICA File Signing" to "Not configured."

  Note: Fix #LC5338 works with StoreFront 3.9 and later versions.

  [#LC5338]

- The icon color for Citrix Receiver for Windows does not change after modifying the StoreFront theme.

  [#LC6435]

- After installing StoreFront 3.0.1000 or 3.0.2000, the management console fails to start and the following error message appears: "The Management console is unavailable because of a root certificate missing, go to verisign and download the certificate - Verisign class primary CA - G5." For more information, see Knowledge Center article CTX218815.

  [#LC6471]

- When you select a configured Site during the setup of XenDesktop, a default store might be created in StoreFront that uses the default Authentication Service. If you remove this store, users of Citrix Receiver for Windows cannot add any other stores and the following error message might appear:

  "A protocol error occurred while communicating with the Authentication Service."

[#LC6664]

- Upgrading StoreFront to version 3.0.2000 from version 2.5 fails with Error 1603. For more information, see Knowledge Center article CTX220411.

  [#LC6816]

- Users are unable to see apps and desktops after logging on when one XML broker does not work correctly, even when there are many working XML brokers. The following error message appears.
  "There are no apps or desktops available to you at this time."

  [#LC6928]

- If you configure Self-Service Password Reset (SSPR) for a specific store from the StoreFront console, the configuration applies to all stores, not just to the specific store you selected.

  [#LC6987]

- Attempts to propagate changes to a server group by selecting "Propagate Changes" on the StoreFront console might fail and the following error message appears:

  "Propagation failed on one or more servers."

  [#LC7428]

Known issues

Jun 02, 2017

The following issues are known to exist in this release.

- If the Administrator changes the group policy setting, MaxPasswordAge, the StoreFront default domain service does not reload the new value. In StoreFront, the user may be shown the incorrect "number of days until password expiry". To work around this issue, restart the Citrix default domain service on each StoreFront server to re-read the value.

  [# DNA-41380]

- Users cannot log on to Citrix Receiver for Web if a custom authentication form contains an element with ID=confirmBtn. Users are unable to log on to Citrix Receiver for Web if a StoreFront authentication extension generates a custom authentication form containing an element with ID **confirmBtn**. Workaround: The authentication extension should use a different ID value in the custom form.

  [# 603196, DNA-22593]

- Studio console crashes with an MMC error after clicking StoreFront node for the first time. After the XenDesktop installation completes and you open the Studio console (and do not close it) and click the StoreFront node in the left pane for the first time, the MMC snap-in might crash. Workaround: Reopen Studio.

  [#655031, DNA-40366]

- Reconnecting apps in the Chrome browser might fail. When using the Chrome browser and reconnecting to published applications from XenApp and XenDesktop servers, clicking **Connect** for the applications might only reconnect the first session when more than one session is being used. Workaround: Click **Connect** again to reconnect each additional session being used.

  [# 575364, DNA-22561]

- Apps in AppController. Apps published in AppController might not start. Workaround: Use the StoreFront PowerShell commands to manually create a store with an authentication service located at **http://***sfserver***/Citrix/Authentication.**

  [# 599292]

- Configuration of Optimal HDX routing with old PowerShell cmdlet fails. When attempting to configure Optimal HDX routing with the old PowerShell cmdlet using **Set-DSOptimalGatewayForFarms**, the command fails.

  Workaround:

  1. Configure a global gateway with the settings you want for Optimal HDX routing using the **Add-DSGlobalV10Gateway** command and provide default values for the authentication settings.

  2. Use the **Add-DSStoreOptimalGateway** command to add the optimal gateway configuration.

  Example:
  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

[# 624040]

- Authentication Service problems after upgrade. Upgrades from StoreFront 2.x to 3.x followed by a propagation to the server group might result in an entry for the **pnaAuthenticationStartupModule** being added to the authentication configuration file. Because entries can be added only to authentication services that have been enabled for PNA authentication services and PNA password change, the authentication service cannot start, as it's missing the named start-up module. Workaround: Remove the entry from the authentication configuration file. By default, the configuration file resides at **C:\inetpub\wwwroot\Citrix\<Your_Auth_Service>\web.config**.

  [# 640644]

サードパーティ製品についての通知

May 22, 2017

StoreFrontには、次のドキュメントで定義された条件の元でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります。

- StoreFrontのサードパーティ製品についての通知

System requirements

May 22, 2017

When planning your installation, Citrix recommends that you allow at least an additional 2 GB of RAM for StoreFront over and above the requirements of any other products installed on the server. The subscription store service requires a minimum of 5 MB disk space, plus approximately 8 MB for every 1000 application subscriptions. All other hardware specifications must meet the minimum requirements for the installed operating system.

Citrix has tested and provides support for StoreFront installations on the following platforms:

- Windows Server 2016 Datacenter and Standard editions
- Windows Server 2012 R2 Datacenter and Standard editions
- Windows Server 2012 Datacenter and Standard editions
- Windows Server 2008 R2 Service Pack 1 Enterprise and Standard editions

Upgrading the operating system version on a server running StoreFront is not supported. Citrix recommends that you install StoreFront on a new installation of the operating system. All the servers in a multiple server deployment must run the same operating system version with the same locale settings. StoreFront server groups containing mixtures of operating system versions and locales are not supported. While a server group can contain a maximum of six servers, from a capacity perspective based on simulations, there is no advantage of server groups containing more than three servers. All servers in a server group must reside in the same location.

Microsoft Internet Information Services (IIS) and Microsoft .NET Framework are required on the server. If either of these prerequisites is installed but not enabled, the StoreFront installer enables them before installing the product. Windows PowerShell and Microsoft Management Console, which are both default components of Windows Server, must be installed on the web server before you can install StoreFront. The relative path to StoreFront in IIS must be the same on all the servers in a group.

The StoreFront installer will add the IIS features it requires. If you pre-install these features, below is the required list:

On all platforms:

- 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

On Windows Server 2008 R2:

- Web-Asp-Net
- As-Tcp-PortSharing

On Windows Server 2012 R2:

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

On Windows Server 2016
- Web-Asp-Net45
- Net-Wcf-Tcp-PortSharing45

StoreFront uses the following ports for communications. Ensure your firewalls and other network devices permit access to these ports.

- TCP ports 80 and 443 are used for HTTP and HTTPS communications, respectively, and must be accessible from both inside and outside the corporate network.
- TCP port 808 is used for communications between StoreFront servers and must be accessible from inside the corporate network.
- A TCP port randomly selected from all unreserved ports is used for communications between the StoreFront servers in a server group. When you install StoreFront, a Windows Firewall rule is configured enabling access to the StoreFront executable. However, since the port is assigned randomly, you must ensure that any firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.
- TCP port 8008 is used by Citrix Receiver for HTML5, where enabled, for communications from local users on the internal network to the servers providing their desktops and applications.

StoreFront supports both pure IPv6 networks and dual-stack IPv4/IPv6 environments.

Citrix has tested and provides support for StoreFront when used with the following Citrix product versions.

Citrix server requirements

StoreFront stores aggregate desktops and applications from the following products.

- XenDesktop
  - XenDesktop 7.14
  - XenDesktop 7.13
  - XenDesktop 7.12
  - XenDesktop 7.11
  - XenDesktop 7.9
  - XenDesktop 7.8
  - XenDesktop 7.7
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
  - XenDesktop 5.6 Feature Pack 1
  - XenDesktop 5.6
  - XenDesktop 5.5
- XenApp
  - XenApp 7.14
  - XenApp 7.13

- XenApp 7.12
- XenApp 7.11
- XenApp 7.9
- XenApp 7.8
- XenApp 7.7
- XenApp 7.6
- XenApp 7.5
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2
- XenApp 6.5 for Windows Server 2008 R2
- XenApp 6.0 for Windows Server 2008 R2

- XenMobile
  - XenMobile 9.0/App Controller 9.0

NetScaler Gateway requirements

The following versions of NetScaler Gateway can be used to provide access to StoreFront for users on public networks.

- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 Build 69.4 (the version number is displayed at the top of the configuration utility)

Citrix Receiver for HTML5 requirements

If you plan to enable users to access desktops and applications using Citrix Receiver for HTML5 running on Receiver for Web sites, the following additional requirements apply.

For internal network connections, Citrix Receiver for HTML5 enables access to desktops and applications provided by the following products.

- XenDesktop 7.14
- XenDesktop 7.13
- XenDesktop 7.12
- XenDesktop 7.11
- XenDesktop 7.9
- XenDesktop 7.8
- XenDesktop 7.7
- XenDesktop 7.6
- XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 7.14
- XenApp 7.13
- XenApp 7.12
- XenApp 7.11
- XenApp 7.9
- XenApp 7.8

- XenApp 7.7
- XenApp 7.6
- XenApp 7.5
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2 (requires Hotfix XA650R01W2K8R2X64051, which is available at http://support.citrix.com/article/CTX135757)

For remote users outside the corporate network, Citrix Receiver for HTML5 enables access to desktops and applications through the following versions of NetScaler Gateway.

- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.1
- Access Gateway 10 Build 71.6014 (the version number is displayed at the top of the configuration utility)

For users connecting through NetScaler Gateway, Citrix Receiver for HTML5 enables access to desktops and applications provided by the following products.

- XenDesktop
  - XenDesktop 7.14
  - XenDesktop 7.13
  - XenDesktop 7.12
  - XenDesktop 7.11
  - XenDesktop 7.9
  - XenDesktop 7.8
  - XenDesktop 7.7
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7
  - XenDesktop 5.6
  - XenDesktop 5.5
- XenApp
  - XenApp 7.14
  - XenApp 7.13
  - XenApp 7.12
  - XenApp 7.11
  - XenApp 7.9
  - XenApp 7.8
  - XenApp 7.7
  - XenApp 7.6
  - XenApp 7.5
  - XenApp 6.5 Feature Pack 2
  - XenApp 6.5 Feature Pack 1 for Windows Server 2008 R2
  - XenApp 6.5 for Windows Server 2008 R2
  - XenApp 6.0 for Windows Server 2008 R2

Updated: 2017-02-22

StoreFront provides a number of different options for users to access their desktops and applications. Citrix Receiver users can either access stores through Citrix Receiver or use a web browser to log on to a Citrix Receiver for Web site for the store. For users who cannot install Citrix Receiver, but have an HTML5-compatible web browser, you can provide access to desktops and applications directly within the web browser by enabling Citrix Receiver for HTML5 on your Citrix Receiver for Web site.

Users with non-domain-joined desktop appliances access their desktops through their web browsers, which are configured to access Desktop Appliance sites. In the case of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with older Citrix clients that cannot be upgraded, users must connect through the XenApp Services URL for the store.

If you plan to deliver offline applications to users, the Offline Plug-in is required in addition to Citrix Receiver for Windows. If you want to deliver Microsoft Application Virtualization (App-V) sequences to users, a supported version of the Microsoft Application Virtualization Desktop Client is also required. For more information, see Managing Streamed Applications. Users cannot access offline applications or App-V sequences through Citrix Receiver for Web sites.

It is assumed that all user devices meet the minimum hardware requirements for the installed operating system.

Requirements for Citrix Receiver-enabled stores

The following Citrix Receiver versions can be used to access StoreFront stores from both internal network connections and through NetScaler Gateway. Connections through NetScaler Gateway can be made using both the NetScaler Gateway Plug-in and/or clientless access. Citrix Receiver for Windows 4.3 is the minimum version required to receive the full StoreFront unified Citrix Receiver experience. See Support for the unified Citrix Receiver experience.

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

Requirements for access to stores through Citrix Receiver for Web sites

The following Citrix Receiver, operating system, and web browser combinations are recommended for users to access Citrix Receiver for Web sites from both internal network connections and through NetScaler Gateway. Connections through NetScaler Gateway can be made using both the NetScaler Gateway Plug-in and clientless access.

- Citrix Receiver for Windows 4.7, Citrix Receiver for Windows 4.6, Citrix Receiver for Windows 4.5, Citrix Receiver for Windows 4.4, Citrix Receiver for Windows 4.3, and Citrix Receiver for Windows 4.2.x
  - Windows 10 (32-bit and 64-bit editions)
    - Microsoft Edge
    - Internet Explorer 11
    - Google Chrome
    - Mozilla Firefox
  - Windows 8.1 (32-bit and 64-bit editions)
    - Internet Explorer 11 (32-bit mode)
    - Google Chrome
    - Mozilla Firefox

- Windows 8 (32-bit and 64-bit editions)
  - Internet Explorer 10 (32-bit mode)
  - Google Chrome
  - Mozilla Firefox
- Windows 7 Service Pack 1 (32-bit and 64-bit editions)
  - Internet Explorer 11, 10, 9
  - Google Chrome
  - Mozilla Firefox
- Windows Embedded Standard 7 Service Pack 1 or Windows Thin PC
  - Internet Explorer 11, 10, 9

- Citrix Receiver for Windows 4.0 and Citrix Receiver for Windows 3.4
  - Windows 8 (32-bit and 64-bit editions)
    - Internet Explorer 10 (32-bit mode)
    - Google Chrome
    - Mozilla Firefox
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions)
    - Internet Explorer 11, 10, 9
    - Google Chrome
    - Mozilla Firefox
  - Windows Embedded Standard 7 Service Pack 1 and Windows Thin PC
    - Internet Explorer 11, 10, 9
- Citrix Receiver for Mac 12.0
  - Mac OS X 10.11 El Capitan
    - Safari 9
    - Google Chrome
    - Mozilla Firefox
  - Mac OS X 10.10 Yosemite
    - Safari 8
    - Google Chrome
    - Mozilla Firefox
  - Mac OS X 10.9 Mavericks
    - Safari 7
    - Google Chrome
    - Mozilla Firefox
- Citrix Receiver for Linux 12.1 and Citrix Receiver for Linux 13.x
  - Ubuntu 12.04 (32-bit) and 14.04 LTS (32-bit)
    - Google Chrome
    - Mozilla Firefox

Requirements for access to desktops and applications through Receiver for HTML5

The following operating systems and web browsers are recommended for users to access desktops and applications using Receiver for HTML5 running on Receiver for Web sites. Both internal network connections and connections through NetScaler Gateway are supported. However, for connections from the internal network, Receiver for HTML5 only enables access to resources provided by specific products. Additionally, specific versions of NetScaler Gateway are required to enable connections from outside the corporate network. For more information, see Infrastructure requirements.

- Browsers
  - Microsoft Edge
  - Internet Explorer 11 and 10 (HTTP connections only)
  - Safari 7
  - Safari 6
  - Google Chrome
  - Mozilla Firefox
- Operating systems
  - Windows RT
  - Windows 10 (32-bit and 64-bit editions)
  - Windows 8.1 (32-bit and 64-bit editions)
  - Windows 8 (32-bit and 64-bit editions)
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions)
  - Windows Vista Service Pack 2 (32-bit and 64-bit editions)
  - Windows Embedded XP
  - Mac OS X 10.10 Yosemite
  - Mac OS X 10.9 Mavericks
  - Mac OS X 10.8 Mountain Lion
  - Mac OS X 10.7 Lion
  - Mac OS X 10.6 Snow Leopard
  - Google Chrome OS 48
  - Google Chrome OS 47
  - Ubuntu 12.04 (32-bit)

Requirements for access to stores through Desktop Appliance sites

The following Citrix Receiver, operating system, and web browser combinations are recommended for users to access Desktop Appliance sites from the internal network. Connections through NetScaler Gateway are not supported.

- Citrix Receiver for Windows 4.5, Citrix Receiver for Windows 4.4, Citrix Receiver for Windows 4.3, and Citrix Receiver for Windows 4.2.x, and Citrix Receiver for Windows 4.1
  - Windows 8.1 (32-bit and 64-bit editions)
    - Internet Explorer 11 (32-bit mode)
  - Windows 8 (32-bit and 64-bit editions)
    - Internet Explorer 10 (32-bit mode)
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions), Windows Embedded Standard 7 Service Pack 1, or Windows Thin PC
    - Internet Explorer 9 (32-bit mode)
    - Internet Explorer 8 (32-bit mode)
  - Windows Embedded XP
    - Internet Explorer 8 (32-bit mode)
- Citrix Receiver for Windows 4.0 or Citrix Receiver for Windows 3.4
  - Windows 8 (32-bit and 64-bit editions)
    - Internet Explorer 10 (32-bit mode)
  - Windows 7 Service Pack 1 (32-bit and 64-bit editions), Windows Embedded Standard 7 Service Pack 1, or Windows Thin PC
    - Internet Explorer 9 (32-bit mode)

        - Internet Explorer 8 (32-bit mode)
    - Windows Embedded XP
        - Internet Explorer 8 (32-bit mode)
- Citrix Receiver for Windows Enterprise 3.4
    - Windows 7 Service Pack 1 (32-bit and 64-bit editions), Windows Embedded Standard 7 Service Pack 1, or Windows Thin PC
        - Internet Explorer 9 (32-bit mode)
        - Internet Explorer 8 (32-bit mode)
    - Windows Embedded XP
        - Internet Explorer 8 (32-bit mode)
- Citrix Receiver for Linux 12.1
    - Ubuntu 12.04 (32-bit)
        - Mozilla Firefox 27

Requirements for access to stores through XenApp Services URLs

All the versions of Citrix Receiver listed above can be used to access StoreFront stores with reduced functionality through XenApp Services URLs. In addition, you can use the older client that does not support other access methods - Citrix Receiver for Linux 12.0 (internal network connections only) - to access stores through XenApp Services URLs. Connections through NetScaler Gateway, where supported, can be made using both the NetScaler Gateway Plug-in and clientless access.

Smart card requirements

Requirement for using Citrix Receiver for Windows 4.X with smart cards

Citrix tests for compatibility with the U.S. Government Dept. Of Defense Common Access Card (CAC), U.S. National Institute of Standards and Technology Personal Identity Verification (NIST PIV) cards, and some USB smart card tokens. You can use contact card readers that comply with the USB Chip/Smart Card Interface Devices (CCID) specification and are classified by the German Zentraler Kreditausschuss (ZKA) as Class 1 smart card readers. ZKA Class 1 contact card readers require that users insert their smart cards into the reader. Other types of smart card readers, including Class 2 readers (which have keypads for entering PINs), contactless readers, and virtual smart cards based on Trusted Platform Module (TPM) chips, are not supported.

For Windows devices, smart card support is based on Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. As a minimum requirement, smart cards and card readers must be supported by the operating system and have received Windows Hardware Certification.

For more information about Citrix-compatible smart cards and middleware, see Smart cards in the XenApp and XenDesktop documentation, and http://www.citrix.com/ready.

Requirements for using Desktop Appliance sites with smart cards

For users with desktop appliances and repurposed PCs running the Citrix Desktop Lock, Citrix Receiver for Windows Enterprise 3.4 is required for smart card authentication. On all other Windows devices, Citrix Receiver for Windows 4.1 can be used.

Requirements for authentication through NetScaler Gateway

The following versions of NetScaler Gateway can be used to provide access to StoreFront for users on public networks

authenticating with smart cards.

- NetScaler Gateway 11.x
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 Build 69.4 (the version number is displayed at the top of the configuration utility)

Plan your StoreFront deployment

May 22, 2017

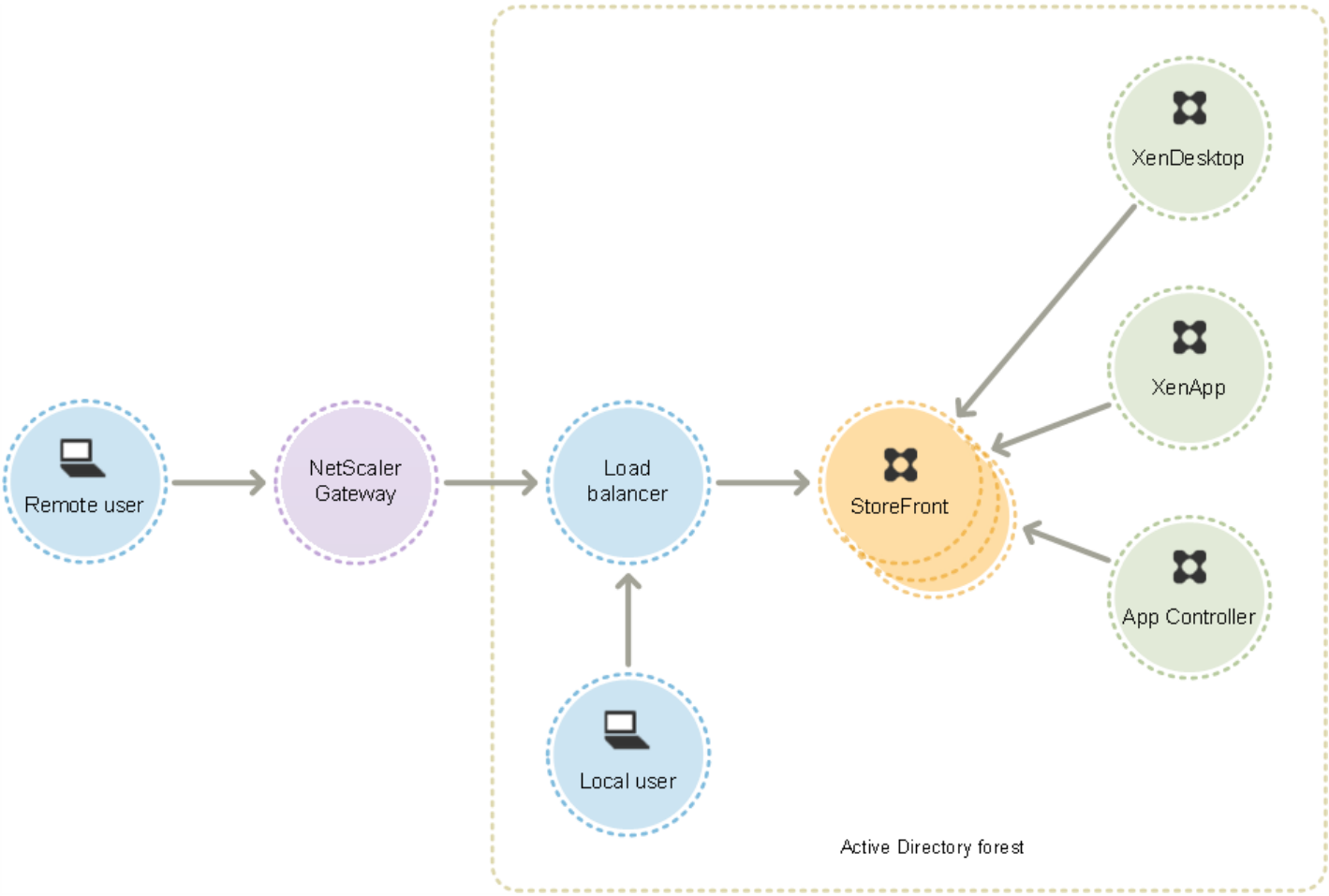
StoreFront employs Microsoft .NET technology running on Microsoft Internet Information Services (IIS) to provide enterprise app stores that aggregate resources and make them available to users. StoreFront integrates with your XenDesktop, XenApp, and App Controller deployments, providing users with a single, self-service access point for their desktops and applications.

StoreFront comprises the following core components:

- The authentication service authenticates users to Microsoft Active Directory, ensuring that users do not need to log on again to access their desktops and applications. For more information, see User authentication.
- Stores enumerate and aggregate desktops and applications from XenDesktop, XenApp, and App Controller. Users access stores through Citrix Receiver, Citrix Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs. For more information, see User access options.
- The subscription store service records details of users' application subscriptions and updates their devices to ensure a consistent roaming experience. For more information about enhancing the experience for your users, see Optimize the user experience.

StoreFront can be configured either on a single server or as a multiple server deployment. Multiple server deployments not only provide additional capacity, but also greater availability. The modular architecture of StoreFront ensures that configuration information and details of users' application subscriptions are stored on and replicated between all the servers in a server group. This means that if a StoreFront server becomes unavailable for any reason, users can continue to access their stores using the remaining servers. Meanwhile, the configuration and subscription data on the failed server are automatically updated when it reconnects to the server group. Subscription data is updated when the server comes back online but you must propagate configuration changes if any were missed by the server while offline. In the event of a hardware failure that requires replacement of the server, you can install StoreFront on a new server and add it to the existing server group. The new server is automatically configured and updated with users' application subscriptions when it joins the server group.

The figure shows a typical StoreFront deployment.



For multiple server deployments, external load balancing through, for example, NetScaler or Windows Network Load Balancing is required. Configure the load balancing environment for failover between servers to provide a fault-tolerant deployment. For more information about load balancing with NetScaler, see Load Balancing. For more information about Windows Network Load Balancing, see http://technet.microsoft.com/en-us/library/hh831698.aspx.

Active load balancing of requests sent from StoreFront to XenDesktop sites and XenApp farms is recommended for deployments with thousands of users or where high loads occur, such as when a large number of users log on over a short period of time. Use a load balancer with built-in XML monitors and session persistency, such as NetScaler.

If you deploy SSL-terminating load balancer or if you need to troubleshoot, you can use the PowerShell cmdlet **Set-STFWebReceiverCommunication**.

Syntax:

Set-STFWebReceiverCommunication [-WebReceiverService] <WebReceiverService> [[-Loopback] <On | Off | OnUsingHttp>] [[-LoopbackPortUsingHttp] <Int32>]

The valid values are:

- **On** - This is the default value for new Citrix Receiver for Web sites. Citrix Receiver for Web uses the schema (HTTPS or HTTP) and port number from the base URL but replaces the host with the loopback IP address to communicate with

StoreFront Services. This works for single server deployments and deployments with a non SSL-terminating load balancer.

- **OnUsingHttp** - Citrix Receiver for Web uses HTTP and the loopback IP address to communicate with StoreFront Services. If you are using an SSL-terminating load balancer, select this value. You must also specify the HTTP port if it is not the default port 80.
- **Off** - This turns off loopback and Citrix Receiver for Web uses the StoreFront base URL to communicate with StoreFront Services. If you perform an in-place upgrade, this is the default value to avoid disruption to your existing deployment.

For example, if you are using an SSL-terminating load balancer, your IIS is configured to use port 81 for HTTP and the path of your Citrix Receiver for Web site is /Citrix/StoreWeb, you can run the following command to configure the Citrix Receiver for Web site:

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

Note that you have to switch off loopback to use any web proxy tool like Fiddler to capture the network traffic between Citrix Receiver for Web and StoreFront Services.

For single server deployments you can install StoreFront on a non-domain-joined server (but certain functionality will be unavailable); otherwise, StoreFront servers must reside either within the Active Directory domain containing your users' accounts or within a domain that has a trust relationship with the user accounts domain unless you enable delegation of authentication to the XenApp and XenDesktop sites or farms. All the StoreFront servers in a group must reside within the same domain.

In a production environment, Citrix recommends using HTTPS to secure communications between StoreFront and users' devices. To use HTTPS, StoreFront requires that the IIS instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications. You can change from HTTP to HTTPS at any time, provided the appropriate IIS configuration is in place.

If you plan to enable access to StoreFront from outside the corporate network, NetScaler Gateway is required to provide secure connections for remote users. Deploy NetScaler Gateway outside the corporate network, with firewalls separating NetScaler Gateway from both the public and internal networks. Ensure that NetScaler Gateway is able to access the Active Directory forest containing the StoreFront servers.

StoreFront enables you to deploy different Stores in different IIS websites per Windows server so that each store can have a different host name and certificate binding.

Start by creating two websites, in addition to the default web site. After creating multiple websites in IIS, use the PowerShell SDK to create a StoreFront deployment in each of those IIS websites. For more information about creating websites in IIS, see How to set up your first IIS Website.

Note: The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront management console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all

instances of PowerShell before opening the StoreFront console.

Example: To create two IIS website deployments - one for applications and one for desktop.

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

StoreFront disables the management console when it detects multiple sites and displays a message to that effect.

For more information, see Before installing and configuring.

The number of Citrix Receiver users supported by a StoreFront server group depends on the hardware you use and on the level of user activity. Based on simulated activity where users log on, enumerate 100 published applications, and start one resource, expect a single StoreFront server with the minimum recommended specification of two virtual CPUs running on an underlying dual Intel Xeon L5520 2.27Ghz processor server to enable up to 30,000 user connections per hour.

Expect a server group with two similarly configured servers in the group to enable up to 60,000 user connections per hour; three nodes up to 90,000 connections per hour; four nodes up to 120,000 connections per hour; five nodes up to 150,000 connections per hour; six nodes up to 175,000 connections per hour.

The throughput of a single StoreFront server can also be increased by assigning more virtual CPUs to the system, with four virtual CPUs enabling up to 55,000 user connections per hour and eight virtual CPUs enabling 80,000 connections per hour.

The minimum recommended memory allocation for each server is 4GB. When using Citrix Receiver for Web, assign an additional 700 bytes per resource, per user in addition to the base memory allocation. As with using Web Receiver, when using Citrix Receiver, design environments to allow an extra 700 bytes per resource, per user on top of the base 4 GB memory requirements for this version of StoreFront.

As your usage patterns might be different than those simulated above, your servers might support more or fewer numbers of users connections per hour.

Important: All servers in a server group must reside in the same location. StoreFront server groups containing mixtures of operating system versions and locales are not supported.

Occasionally, network issues or other problems can occur between a StoreFront store and the servers that it contacts, causing delays or failures for users. You can use the timeout settings for a store to tune this behavior. If you specify a short timeout setting, StoreFront quickly abandons a server and tries another one. This is useful if, for example, you have configured multiple servers for failover purposes.

If you specify a longer timeout, StoreFront waits longer for a response from a single server. This is beneficial in environments where network or server reliability is uncertain and delays are common.

Citrix Receiver for Web also has a timeout setting, which controls how long a Citrix Receiver for Web site waits for a response from the store. Set this timeout setting to a value at least as long as the store timeout. A longer timeout setting allows for better fault tolerance, but users might experience long delays. A shorter timeout setting reduces delays for users, but they might experience more failures.

For information about setting timeouts, see Communication time-out duration and server retry attempts and Communication time-out duration and retry attempts.

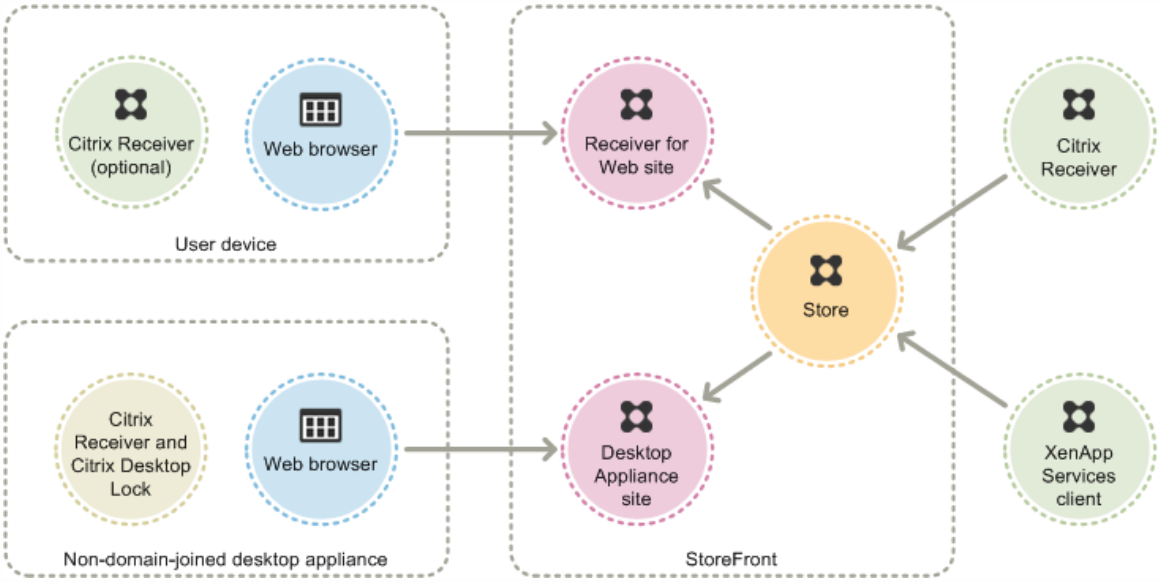
ユーザーアクセスのオプション

May 22, 2017

ユーザーは、以下の4つの方法でStoreFrontストアにアクセスできます。

- Citrix Receiver - 適切なバージョンのCitrix Receiverのユーザーは、Citrix Receiverのユーザーインターフェイスから StoreFrontストアにアクセスできます。Citrix Receiverからストアに透過的にアクセスできるため、最も簡単であり、より多くの機能が提供されます。
- Citrix Receiver for Webサイト - 適切なバージョンのWebブラウザーのユーザーは、Citrix Receiver for WebサイトからStoreFrontストアにアクセスすることができます。デフォルトでは、デスクトップとアプリケーションにアクセスするために、適切なバージョンのCitrix Receiverも必要です。ただし、管理者は、Citrix ReceiverをインストールできないユーザーがHTML5互換のWebブラウザーからデスクトップやアプリケーションに直接アクセスできるように、Citrix Receiver for Webサイトを構成できます。デフォルトでは、管理者が新しいストアを作成するときにそのストアのCitrix Receiver for Webサイトが作成されます。
- Desktop Applianceサイト - ドメインに参加していないデスクトップアプライアンスのユーザーは、全画面モードのWebブラウザーでデスクトップアプライアンスサイトにアクセスして自分のデスクトップにアクセスします。管理者がCitrix StudioでXenDesktop環境の新しいストアを作成すると、デフォルトでそのストアのデスクトップアプライアンスサイトが作成されます。
- XenApp Services URL - ドメインに参加しているデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトからストアに接続できます。デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。

この図は、ユーザーがStoreFrontストアにアクセスするためのオプションを示しています。



Citrix Receiverのユーザーインターフェイスでストアにアクセスすると、最良のユーザーエクスペリエンスと多くの機能が提供されます。この方法でストアにアクセスできるCitrix Receiverのバージョンについては、「システム要件」を参照してください。

Citrix Receiverでは、ビーコンポイントとして内部URLおよび外部URLを使用します。これらのビーコンポイントにCitrix Receiverでアクセスできるかどうかにより、ユーザーがローカルに接続されているのかパブリックネットワークに接続されているのかが識別されます。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバー

がそのユーザーの位置情報に基づいて適切な接続詳細をCitrix Receiverに返します。これにより、ユーザーがCitrix Receiverでデスクトップやアプリケーションにアクセスするときに再ログオンする必要がなくなります。詳しくは、「ビーコンポインの構成」を参照してください。

Citrix Receiverをインストールしたら、デスクトップやアプリケーションのストアに接続するための構成を行う必要があります。管理者は、次のいずれかの方法を使用してユーザーによる構成操作を簡略化できます。

重要：デフォルトでは、Citrix ReceiverはストアへのHTTPSを必要とします。StoreFrontがHTTPS用に構成されていない場合、Citrix ReceiverでHTTP接続が使用されるようにユーザーが構成を変更する必要があります。実稼働環境では、StoreFrontへのすべてのユーザー接続が保護されるようにしてください。詳しくは、「*コマンドラインパラメーターを使用したCitrix Receiver for Windows*の構成とインストール」を参照してください。

プロビジョニングファイル

管理者は、ストアへの接続情報が定義されたプロビジョニングファイルをユーザーに提供します。Citrix Receiverをインストールした後で、提供されたCRファイルをユーザーが開くと、ストアのアカウントが自動的に構成されます。Citrix Receiver for Webサイトのデフォルトでは、そのサイトの単一ストア用のプロビジョニングファイルがユーザーに提供されます。管理者は、使用する各ストアのReceiver for Webサイトからプロビジョニングファイルをダウンロードするようユーザーに指示します。また、ユーザーの設定をより詳細に管理するには、Citrix StoreFront管理コンソールで特定のストアの接続情報を定義したプロビジョニングファイルを生成できます。その後で、それらのファイルを適切なユーザーに配布します。詳しくは、「ユーザーに対するストアプロビジョニングファイルのエクスポート」を参照してください。

セットアップURLの自動生成

Mac OSのユーザーには、Citrix Receiver for Mac Setup URL Generatorを使ってストアの接続情報を含んでいるセットアップURLを生成し、それをユーザーに提供できます。ユーザーがCitrix Receiverをインストールした後で、管理者から提供されたURLをクリックするとストアのアカウントが自動的に構成されます。管理者は、Citrix Receiver for Mac Setup URL Generatorで展開環境の詳細を入力してURLを生成し、そのURLをユーザーに配布します。

ユーザーによる構成

ユーザーがCitrix Receiverの構成に慣れている場合は、自分でストアのURLを入力して新しいアカウントを作成できます。NetScaler Gateway 10.1またはAccess Gateway 10経由でStoreFrontにアクセスするリモートユーザーは、そのゲートウェイアプライアンスのURLを入力します。Citrix Receiverでの初回接続時に、アカウントの構成に必要な情報が取得されます。Access Gateway 9.3経由で接続するユーザーは、自分でアカウントをセットアップすることはできません。上記のいずれかの方法を使用する必要があります。詳しくは、Citrix Receiverのドキュメントを参照してください。

メールアドレスによるアカウント検出

Citrix Receiverをデバイスに初めてインストールするユーザーは、Citrix社のWebサイトまたは内部ネットワーク上のダウンロードページからCitrix Receiverをダウンロードして、自分のメールアドレスを入力してアカウントをセットアップできます。管理者は、Microsoft Active Directory DNS（Domain Name System：ドメイン名システム）サーバー上でNetScaler GatewayまたはStoreFrontに対するサービスロケーション（SRV）ロケーターリソースレコードを構成します。ユーザーはストアへのアクセス情報を知っている必要はありません。代わりに、Citrix Receiverの初回構成時に自分のメールアドレスを入力します。Citrix Receiverはメールアドレスで指定されたドメインのDNSサーバーにアクセスして、SRVリソースレコードに追加されている詳細を取得します。これにより、アクセスできるストアの一覧がCitrix Receiverに表示されます。

メールアドレスによるアカウント検出を有効にすると、デバイスにCitrix Receiverを新規インストールしたユーザーが、自分のメールアドレスを入力することでアカウントを自動的にセットアップできます。ユーザーがCitrix ReceiverをCitrix社のWebサ

イトまたは内部ネットワーク上のダウンロードページからダウンロードする場合は、ユーザーがストアへのアクセス方法を知っていなくてもCitrix Receiverをインストールして構成できます。Citrix ReceiverをReceiver for Webサイトなどのほかの場所からダウンロードする場合は、メールアドレスによるアカウント検出を使用できます。Citrix Receiver for WebからダウンロードしたReceiverWeb.exeまたはReceiverWeb.dmgでは、ストアの構成は求められません。この場合も、ユーザーは［アカウントの追加］を使用してメールアドレスを入力できます。

Citrix Receiverの初回構成時に、ユーザーのメールアドレスまたはストアのURLを入力するためのダイアログボックスが開きます。ユーザーがメールアドレスを入力すると、Citrix Receiverはメールアドレスで指定されたドメインのMicrosoft Active Directory DNS（Domain Name System：ドメイン名システム）サーバーにアクセスして、ユーザーが選択可能なストアの一覧を取得します。

Citrix Receiverでユーザーのメールアドレスからストアを検索できるようにするには、DNSサーバー上でNetScaler GatewayまたはStoreFrontに対するサービスロケーション（SRV）ロケーターリソースレコードを構成します。また、フォールバックとして「discoverReceiver. domain」という名前のサーバーにStoreFrontを展開することもできます（ここではユーザーのメールアカウントのドメインです）。指定されたドメインにSRVレコードが見つからない場合、Citrix Receiverは「discoverReceiver」という名前のマシンを検索してStoreFrontサーバーを検出します。

メールアドレスによるアカウント検出を有効にするには、NetScaler GatewayアプライアンスまたはStoreFrontサーバー上に有効なサーバー証明書をインストールする必要があります。ルート証明書へのチェーンのすべてが有効である必要もあります。ユーザーエクスペリエンスを向上させるには、サブジェクトまたはサブジェクトの別名（SAN：Subject Alternative Name）エントリがdiscoverReceiver.domainである証明書をインストールします（ここで<domain>はユーザーのメールアカウントのドメインです）。このドメインのワイルドカード証明書を使用することもできますが、そのような証明書の使用が社内のセキュリティポリシーで許可されていることを確認してください。ユーザーのメールアカウントを含んでいるドメイン用のほかの証明書を使用することもできますが、ユーザーがCitrix ReceiverでStoreFrontサーバーに最初に接続したときに、証明書に関する警告が表示されます。上記以外の証明書を使用してメールアドレスによるアカウント検出機能を使用することはできません。

社内ネットワークの外から接続するユーザーに対してメールアドレスによるアカウント検出を有効にするには、NetScaler GatewayでStoreFront接続の詳細を構成する必要があります。詳しくは、「Connecting to StoreFront by Using Email-Based Discovery」を参照してください。

SRVレコードのDNSサーバーへの追加

1. Windowsの［**スタート**］画面で［**管理ツール**］をクリックして、［**管理ツール**］フォルダーの［**DNS**］をクリックします。
2. **DNSマネージャー**の左側のペインで、前方参照ゾーンまたは逆引き参照ゾーンのドメインを選択します。ドメインを右クリックして［**その他の新しいレコード**］を選択します。
3. ［**リソースレコードの種類**］ダイアログボックスで、［**サービスロケーション（SRV）**］を選択して［**レコードの作成**］をクリックします。
4. ［**新しいリソースレコード**］ダイアログボックスで、［**サービス**］ボックスにホスト値の**_citrixreceiver**を入力します。
5. ［**プロトコル**］ボックスに、値**_tcp**を入力します。
6. ［**このサービスを提供しているホスト**］ボックスに、NetScaler Gatewayアプライアンス（ローカルおよびリモートのユーザーをサポートする場合）またはStoreFrontサーバー（ローカルユーザーのみをサポートする場合）の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）とポートを*servername.domain:port*形式で入力します。
   環境内に内部DNSサーバーと外部DNSサーバーの両方がある場合は、内部DNSサーバー上にStoreFrontサーバーFQDNのSRVレコードを追加し、外部DNSサーバー上にNetScaler Gateway FQDNの別のSRVレコードを追加できます。この構成により、リモートユーザーにはNetScaler Gatewayの接続情報が提供され、ローカルユーザーにはStoreFrontの接続情報が提供されます。
7. NetScaler GatewayアプライアンスにSRVレコードを構成した場合、セッションプロファイルまたはグローバル設定で

StoreFront接続の詳細をNetScaler Gatewayに追加します。

適切なバージョンのWebブラウザーのユーザーは、Citrix Receiver for WebサイトからStoreFrontストアにアクセスすることができます。管理者が新しいストアを作成すると、そのストアのCitrix Receiver for Webサイトが自動的に作成されます。Citrix Receiver for Webサイトのデフォルト構成では、デスクトップとアプリケーションにアクセスするために、ユーザーが適切なバージョンのCitrix Receiverをインストールする必要があります。Citrix Receiver for WebサイトでサポートされるCitrix ReceiverとWebブラウザーのバージョンについて詳しくは、「ユーザーデバイスの要件」を参照してください。

デフォルトでは、ユーザーがWindowsまたはMac OS Xが動作するコンピューターからCitrix Receiver for Webサイトにアクセスすると、Citrix Receiverがユーザーデバイスにインストール済みであるかどうかが判別されます。Citrix Receiverが検出されない場合は、プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページが開きます。デフォルトのダウンロード元はCitrix社のWebサイトですが、StoreFrontサーバーにインストールファイルをコピーして、ユーザーにこれらのローカルファイルを提供することもできます。Citrix Receiverのインストールファイルをローカルに保存すると、古いバージョンのクライアントを使用しているユーザーに対して、StoreFrontサーバー上のCitrix Receiverにアップグレードするためのオプションを提供することもできます。Citrix Receiver for WindowsおよびCitrix Receiver for Macの展開を構成する方法について詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

Citrix Receiver for HTML5

Citrix Receiver for HTML5はStoreFrontのコンポーネントであり、デフォルトでCitrix Receiver for Webサイトに統合されています。Citrix Receiver for WebサイトのCitrix Receiver for HTML5を有効にすると、Citrix Receiverをインストールできないユーザーもリソースにアクセスできるようになります。Citrix Receiver for HTML5を使用すると、デスクトップやアプリケーションにHTML5互換のWebブラウザーからアクセスできます。デバイスにCitrix Receiverをインストールする必要はありません。サイトのCitrix Receiver for HTML5は、デフォルトで無効になります。Citrix Receiver for HTML5の有効化について詳しくは、citrix-receiver-download-page-template.htmlを参照してください。

Citrix Receiver for HTML5でデスクトップやアプリケーションにアクセスするには、HTML5互換のWebブラウザーでCitrix Receiver for Webサイトを開きます。Citrix Receiver for HTML5でサポートされるオペレーティングシステムとWebブラウザーについて詳しくは、「ユーザーデバイスの要件」を参照してください。

Citrix Receiver for HTML5は、内部ネットワーク上のユーザーとNetScaler Gateway経由で接続するリモートユーザーの両方が使用できます。内部ネットワークからの接続の場合、Citrix Receiver for HTML5では、Citrix Receiver for Webサイトでサポートされる一部の製品で配信されるデスクトップおよびアプリケーションへのアクセスのみがサポートされます。管理者がStoreFrontを構成するときにCitrix Receiver for HTML5をオプションとして選択すると、NetScaler Gateway経由で接続するユーザーがより多くの製品で提供されたリソースにアクセスできるようになります。Citrix Receiver for HTML5を使用する場合は、特定のバージョンのNetScaler Gatewayが必要です。詳しくは、「インフラストラクチャの要件」を参照してください。

デフォルトでは、内部ネットワーク上のローカルユーザーがXenDesktopやXenAppで提供されるリソースにCitrix Receiver for HTML5でアクセスすることはできません。Citrix Receiver for HTML5でデスクトップやアプリケーションへのローカルアクセスを有効にするには、XenDesktopおよびXenAppのサーバー側でポリシーの［ICA WebSockets接続］を有効にする必要があります。ファイアウォールとそのほかのネットワークデバイスで、ポリシーで指定されたCitrix Receiver for HTML5ポートへのアクセスが許可されていることを確認してください。詳しくは、「WebSocketのポリシー設定」を参照してください。

デフォルトでは、Citrix Receiver for HTML5は新しいブラウザータブでデスクトップやアプリケーションを起動します。ただし、ユーザーがCitrix Receiver for HTML5を使用してショートカットからリソースを起動した場合、既存のブラウザータブのCitrix Receiver for Webサイトが置き換わり、そこでデスクトップまたはアプリケーションが起動します。Receiver for Webサイトと同じタブでリソースが常に起動するようにCitrix Receiver for HTML5を構成することもできます。詳しくは、「Citrix

Receiver for HTML5のブラウザータブ使用の構成」を参照してください。

リソースのショートカット

Citrix Receiver for Webサイトからアクセスできるデスクトップやアプリケーションのリンクを生成できます。生成したリンクを内部ネットワーク上でホストされているWebサイトに埋め込んで、ユーザーがすばやくリソースにアクセスできるようにします。ユーザーがリンクをクリックすると、Receiver for Webサイトにリダイレクトされます。ここで、ユーザーがReceiver for Webサイトにログオンしていない場合はログオンします。Citrix Receiver for Webサイトでは、リソースが自動的に起動します。ユーザーがサブスクライブしていないアプリケーションの場合は、自動的にサブスクライブされます。リソースのショートカットの生成について詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

Citrix Receiver for Webサイトからアクセスするデスクトップやアプリケーションと同様に、ショートカットを使用する場合もユーザーがCitrix ReceiverまたはCitrix Receiver for HTML5を使用する必要があります。Citrix Receiver for Webサイトで使用される方法（Citrix ReceiverまたはReceiver for HTML5）は、サイトの構成、Citrix Receiverをユーザーのデバイスで検出できるかどうか、およびHTML5互換のWebブラウザーを使用しているかどうかによって異なります。セキュリティ上の理由により、Internet Explorerユーザーには、ショートカット経由でアクセスしたリソースの起動を確認するメッセージが表示される場合があります。このメッセージが表示されなくなるようにするには、Internet Explorerの［ローカルイントラネット］または［信頼済みサイト］のゾーンにReceiver for Webサイトを追加するようユーザーに指示します。ショートカット経由でCitrix Receiver for Webサイトにアクセスする場合、ワークスペースコントロールとデスクトップの自動起動機能はどちらもデフォルトで無効になります。

アプリケーションのショートカットを生成するときは、Citrix Receiver for Webサイトで配信されているアプリケーションの名前が重複していないことを確認してください。ショートカットでは、同じ名前を持つアプリケーションの複数のインスタンスを区別できません。同様に、単一のデスクトップグループの複数のデスクトップインスタンスをCitrix Receiver for Webサイトで配信する場合、インスタンスごとに異なるショートカットを作成することはできません。ショートカットでは、コマンドラインパラメーターをアプリケーションに渡すことはできません。

アプリケーションのショートカットを生成するには、そのショートカットをホストする内部WebサイトのURLをStoreFrontで一覧に追加します。ユーザーがWebサイト上のショートカットをクリックすると、この一覧が照会され、要求が信頼されるWebサイトからのものであるかどうか確認されます。ただし、NetScaler Gateway経由で接続するユーザーの場合、URLがStoreFrontに渡されないため、ショートカットをホストしているWebサイトは検証されません。信頼される内部Webサイトのショートカットにのみリモートユーザーがアクセスできるようにするには、これらのサイトへのアクセスのみが許可されるようにNetScaler Gatewayを構成します。詳しくは、http://support.citrix.com/article/CTX123610を参照してください。

サイトのカスタマイズ

Citrix Receiver for Webサイトでは、ユーザーインターフェイスをカスタマイズできます。表示される文字列、カスケーディングスタイルシート、およびJavaScriptファイルを編集できます。また、ログオン前やログオフ後にカスタムの画面を表示したり、言語パックを追加したりすることもできます。

重要な注意事項

ユーザーがCitrix Receiver for Webサイトからストアにアクセスする場合、アプリケーションの同期機能など、Citrix Receiver内でのストアへのアクセスでサポートされる多くの機能を使用できます。以下の制限事項を考慮して、Citrix Receiver for Webサイトでユーザーにストアへのアクセスを提供するかどうかを決定してください。

- 1つのCitrix Receiver for Webサイトから複数のストアにアクセスすることはできません。
- Citrix Receiver for Webサイトでは、SSL（Secure Sockets Layer）仮想プライベートネットワーク（VPN）接続を開始できません。VPN接続なしでNetScaler Gatewayを介してログオンしているユーザーは、App ControllerによりVPN接続を要求

されるWebアプリケーションにアクセスできません。
- Citrix Receiver for Webサイトからストアにアクセスする場合、サブスクライブしたアプリケーションはWindowsの[スタート]画面に追加されません。
- Citrix Receiver for Webサイトを経由してアクセスするホストアプリケーションでファイルタイプの関連付けを使用して、ローカルドキュメントを開くことはできません。
- オフラインアプリケーションには、Citrix Receiver for Webサイトからアクセスできません。
- Citrix Receiver for Webサイトでは、ストアに統合したCitrix Online製品はサポートされません。Citrix Receiver for WebサイトからCitrix Online製品にアクセスできるようにするには、App Controllerで配信するか、ホストされるアプリケーションとして公開する必要があります。
- VDAがXenApp 7.6またはXenDesktop 7.6でSSLが有効になっている、またはユーザーがNetScaler Gatewayを使って接続している場合、HTTPS接続でCitrix Receiver for HTML5を使用できます。
- Mozilla FirefoxでHTTPS接続のCitrix Receiver for HTML5を使用するには、Firefoxのアドレスバーに「about:config」と入力し、［network.websocket.allowInsecureFromHTTPS］をtrueに設定します。

ドメイン不参加のデスクトップアプライアンスを使用するユーザーは、デスクトップアプライアンスサイト経由でデスクトップにアクセスできます。ドメイン不参加のデバイスとは、StoreFrontサーバーを含んでいるMicrosoft Active Directoryフォレスト内のドメインに属していないデバイスを意味します。

管理者がCitrix StudioでXenDesktop環境の新しいストアを作成すると、デフォルトでそのストアのデスクトップアプライアンスサイトが作成されます。デスクトップアプライアンスサイトは、StoreFrontがXenDesktopの一部としてインストールおよび構成されている場合にのみデフォルトで作成されます。管理者は、Windows PowerShellコマンドを使用してデスクトップアプライアンスサイトを作成することもできます。詳しくは、「デスクトップアプライアンスサイトの構成」を参照してください。

デスクトップアプライアンスサイトでは、ローカルデスクトップにログオンするときと同じようなユーザーエクスペリエンスが提供されます。デスクトップアプライアンス上のWebブラウザーは、全画面モードで起動して、デスクトップアプライアンスサイトのログオン画面を表示するように構成されます。デフォルトでは、ユーザーがデスクトップアプライアンスサイトにログオンすると、そのユーザーに提供されているデスクトップのうち（アルファベット順で）最初のデスクトップが自動的に起動します。ストアで複数のデスクトップをユーザーに提供する場合は、デスクトップアプライアンスサイトに複数のデスクトップを表示して、ユーザーが選択できるように構成できます。詳しくは、「デスクトップアプライアンスサイトの構成」を参照してください。

デスクトップが起動すると全画面モードで表示され、Webブラウザーは非表示になります。ユーザーは、デスクトップアプライアンスサイトから自動的にログアウトされます。ユーザーがデスクトップからログオフすると、Webブラウザーが再度表示され、デスクトップアプライアンスサイトのログオン画面が開きます。デスクトップが起動すると、デスクトップにアクセスできない場合にデスクトップを再起動するためのリンクを含んでいるメッセージが表示されます。この機能を有効にするには、管理者がデリバリーグループを構成するときにユーザーによるデスクトップの再起動を許可する必要があります。詳しくは、「デリバリーグループ」を参照してください。

デスクトップへのアクセスを提供するには、デスクトップアプライアンス上に適切なバージョンのCitrix Receiverが必要です。通常、XenDesktop互換のアプライアンスベンダーは、Citrix Receiverを自社の製品に統合しています。Windowsアプライアンスの場合は、Citrix Desktop Lockもインストールして、デスクトップアプライアンスサイトのURLを指定する必要があります。Internet Explorerを使用する場合は、［ローカルイントラネット］または［信頼済みサイト］のゾーンにデスクトップアプライアンスサイトを追加する必要があります。Citrix Desktop Lockについて詳しくは、「ユーザーがローカルデスクトップにアクセスできないようにする」を参照してください。

重要な注意事項

デスクトップアプライアンスサイトは、ドメイン不参加のデスクトップアプライアンスからデスクトップにアクセスする内
ネットワーク上のローカルユーザーを対象としています。以下の制限事項を考慮して、デスクトップアプライアンスサイトで
ユーザーにストアへのアクセスを提供するかどうかを決定してください。

- ドメインに参加しているデスクトップアプライアンスや再目的化されたPCを展開する場合は、それらのアプライアンスや
  PCでは、ストアにデスクトップアプライアンスサイト経由でアクセスするように構成しないでください。ストアのXenAp
  ServicesサイトのURLを使用してCitrix Receiverを構成できますが、ドメイン参加および不参加の使用例の両方に、新しい
  Desktop Lockをお勧めします。詳しくは、「Citrix Receiver Desktop Lock」を参照してください。
- デスクトップアプライアンスサイトでは、社内ネットワーク外のリモートユーザーからの接続はサポートされません。
  NetScaler Gatewayにログオンするユーザーは、デスクトップアプライアンスサイトにアクセスできません。

アップグレードできない古いバージョンのCitrixクライアントのユーザーは、クライアントを構成するときにストアのXenApp
ServicesサイトのURLを指定することにより、ストアにアクセスできるようになります。また、管理者は、ドメインに参加し
いるデスクトップアプライアンスのユーザー、およびCitrix Desktop Lockを実行している再目的化されたPCのユーザーが
XenApp Servicesサイト経由でストアにアクセスできるように構成することもできます。ドメインに参加しているデバイスと
は、StoreFrontサーバーを含んでいるActive Directoryフォレスト内のドメインに属しているデバイスを意味します。

StoreFrontでは、Citrix ReceiverからXenApp Servicesサイトへの近接カードを使ったパススルー認証がサポートされます。
Citrix Fast Connect APIを使用するCitrix Readyパートナー製品では、Citrix Receiver for WindowsからXenApp Servicesサイトを
介して効率的にストアにログオンできます。ユーザーは、近接カードを使ってワークステーションにログオンし、
XenDesktopおよびXenAppから提供されるデスクトップやアプリケーションに迅速に接続できます。詳しくは、最新のCitrix
Receiver for Windowsのドキュメントを参照してください。

デフォルトでは、管理者が新しいストアを作成するときに、そのストアのXenApp Services URLが有効になります。ストアの
XenApp Services URLは、http[s]://serveraddress/Citrix/storename/PNAgent/config.xmlという形式になります。ここで、
serveraddressはStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名であり、storenameはストアの作成
時に指定した名前です。これにより、PNAgentプロトコルのみを使用できるCitrix ReceiverがStoreFrontに接続できます。
XenApp Services URLを経由してストアにアクセスできるクライアントについては、「ユーザーデバイスの要件」を参照して
ください。

重要な注意事項

XenApp ServicesサイトのURLは、Citrix Receiverにアップグレードできず、代替のアクセス方法を使用できないユーザーをサ
ポートするために使用されます。以下の制限事項を考慮して、XenApp Servicesサイトでユーザーにストアへのアクセスを提供
するかどうかを決定してください。

- ストアのXenApp Services URLは変更できません。
- 構成ファイルconfig.xmlを編集してXenApp Services URL設定を変更することはできません。
- XenApp Servicesサイトでは、指定ユーザー認証、ドメインパススルー認証、スマートカード認証、スマートカードパス
  ルー認証がサポートされます。デフォルトでは、指定ユーザー認証が有効になります。各XenApp Servicesサイトに構成で
  きる認証方法と各ストアで使用できるXenApp Servicesサイトは、それぞれ1つだけです。複数の認証方法を有効にするに
  は、個別のストアを作成して、それらのXenApp Servicesサイトで異なる認証方法を有効にします。この場合、どのストア
  にアクセスすべきかをユーザーに通知してください。詳しくは、「XML-based authentication」を参照してください。
- XenApp ServicesサイトではワークスペースコントロールがXenApp有効になり、この構成を変更したり無効にしたりすることはで
  きません。
- ユーザーのパスワード変更要求は、StoreFrontの認証サービスを介さず、ストアにデスクトップとアプリケーションを提
  供するXenDesktopおよびXenAppサーバーからドメインコントローラーに直接送信されます。

ユーザー認証

May 22, 2017

StoreFrontではユーザーがストアにアクセスするときにさまざまな認証方法がサポートされますが、ユーザーのアクセス方法とネットワークの場所によっては一部の認証方法を使用できない場合があります。セキュリティ上の理由により、最初のストアの作成時には一部の認証方法がデフォルトで無効になります。ユーザーの認証方法の有効化および無効化について詳しくは、「認証サービスの作成および構成」を参照してください。

ユーザーは、ストアにアクセスするときに、資格情報を入力すると認証されます。デフォルトでは、指定ユーザー認証が有効になります。指定ユーザー認証は、すべてのアクセス方法でサポートされます。

ユーザーがNetScaler Gatewayを使用してCitrix Receiver for Webにアクセスする場合、NetScaler Gatewayによりログオンおよび期限切れパスワードの変更処理が行われます。ユーザーが自分でパスワードを変更する場合は、Citrix Receiver for Webのユーザーインターフェイスを使用します。ユーザーがパスワードを変更するとNetScaler Gatewayセッションが終了します。ユーザーは再ログオンする必要があります。Citrix Receiver for Linuxユーザーは、有効期限切れのパスワードのみを変更できます。

ユーザーはAccess Gatewayにログオンすることによって認証を受け、ストアにアクセスするときは自動的にログオンします。StoreFrontでは、NetScalerを経由することなく社内ネットワーク内でSAML認証を直接サポートすることができます。

SAML（Security Assertion Markup Language：セキュリティアサーションマークアップランゲージ）は、Microsoft AD FS（Active Directoryフェデレーションサービス）などのIDおよび認証製品で採用されている公開標準規格です。StoreFrontとSAML認証を統合することで、管理者はたとえば、ユーザーが一度社内ネットワークへログオンすれば、以降は公開アプリケーションにシングルサインオンできるようにすることができます。

要件：

- 手順5：Citrix Federated Authentication Serviceを再起動します。
- SAML 2.0準拠のIDプロバイダー（IdPs）：
  - SAMLバインドのみを使用するMicrosoft AD FS v4.0（Windows Server 2016）（WSフェデレーションバインドは不可）。詳しくは、Microsoftの「AD FS 2016 Deployment」および「AD FS 2016 Operations」を参照してください。
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2008 R2
  - NetScaler Gateway構成：
- StoreFrontの管理コンソールを使用して、SAML認証を新しい展開環境（「新しい展開環境の作成」を参照）または既存の展開環境（「認証サービスの構成」を参照）で構成します。また、PowerShellコマンドレットを使用してSAML認証を構成することもできます。「StoreFront SDK」を参照してください。
- Citrix Receiver for Windows（4.6以降）またはCitrix Receiver for Web

現在、NetScalerでのSAML認証の使用は、Citrix Receiver for Webサイトでサポートされています。

ユーザーはドメインに参加しているWindowsコンピューターにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。StoreFrontをインストールする際、ドメインパススルー認証はデフォルトで無効になっています。ドメインパススルー認証は、Citrix ReceiverおよびXenApp Servicesサイトからストアに接続するユーザーに対して有効

にすることができます。Citrix Receiver for Webサイトは、Internet Explorerを使用する場合のみドメインパススルー認証をサポートします。管理コンソールのCitrix Receiver for Webサイトのノードでドメインパススルー認証を有効にし、Citrix Receiver for Windows上でSSONを構成する必要があります。Citrix Receiver for HTML5では、ドメイン資格情報のパススルー認証はサポートされません。ドメインパススルー認証を使用するには、ユーザーがCitrix Receiver for WindowsまたはOnline Plug-in for Windowsを使用する必要があります。また、Citrix Receiver for WindowsまたはOnline Plug-in for Windowsをユーザーのデバイスにインストールするときにパススルー認証を有効にする必要があります。

ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。NetScaler Gatewayからのパススルー認証は、ストアへのリモートアクセスを最初に構成するときにデフォルトで有効になります。ユーザーは、Citrix ReceiverまたはCitrix Receiver for Webサイトを使用してNetScaler Gateway経由でストアに接続できます。デスクトップアプライアンスサイトでは、NetScaler Gatewayを経由する接続はサポートされません。NetScaler Gatewayを使用するためのStoreFrontの構成について詳しくは、「NetScaler Gateway接続の追加」を参照してください。

StoreFrontは、次のNetScaler Gateway認証方法でのパススルーをサポートします。

- **セキュリティトークン：**ユーザーは、セキュリティトークンから生成されるトークンコードから得られるパスコードを使用してNetScaler Gatewayにログオンします。トークンコードと暗証番号を組み合わせてパスコードにする場合もあります。セキュリティトークンのみによるパススルー認証を有効にする場合は、ユーザーに提供するリソースでほかの認証方法（Microsoft Active Directoryドメインの資格情報など）が使用されないようにしてください。
- **ドメインおよびセキュリティトークン：**NetScaler Gatewayにログオンするユーザーは、ドメイン資格情報とセキュリティトークンパスコードの両方を入力する必要があります。
- **クライアント証明書：**ユーザーは、NetScaler Gatewayに提示されるクライアント証明書の属性に基づいて認証を受け、NetScaler Gatewayにログオンします。ユーザーがスマートカードを使用してNetScaler Gatewayにログオンできるようにするには、クライアント証明書認証を構成します。クライアント証明書による認証は、ほかの種類の認証と共に2要素認証でも使用できます。

StoreFrontでは、リモートユーザーがストアにアクセスするときに資格情報を再入力しなくて済むように、NetScaler Gatewayの認証サービスを使用してリモートユーザーをパススルー認証します。ただし、デフォルトでは、パスワードを使用してNetScaler Gatewayにログオンするユーザーに対してのみパススルー認証が有効になります。スマートカードユーザーに対してNetScaler GatewayからStoreFrontへのパススルー認証を構成するには、資格情報の検証をNetScaler Gatewayに委任します。詳しくは、「認証サービスの作成と構成」を参照してください。

NetScaler Gateway Plug-inを使用すると、SSL（Secure Sockets Layer）仮想プライベートネットワーク（VPN）トンネルを介したパススルー認証でCitrix Receiver内からストアに直接接続できます。NetScaler Gateway Plug-inをインストールできないリモートユーザーも、パススルー認証によりCitrix Receiver内からストアに接続できます（クライアントレスアクセス）。クライアントレスアクセスを使ってストアに接続するには、クライアントレスアクセスをサポートするバージョンのCitrix Receiverが必要です。

また、Citrix Receiver for Webサイトに対するパススルー認証によるクライアントレスアクセスを有効にできます。これを行うには、セキュアリモートプロキシとして動作するようにNetScaler Gatewayを構成する必要があります。ユーザーはNetScaler Gatewayに直接ログオンして、Citrix Receiver for Webサイトを使用して再認証なしでアプリケーションにアクセスします。

クライアントレスアクセスによりApp Controllerリソースに接続するユーザーは、外部のSaaS（Software-as-a-Service）アプリケーションにのみアクセスできます。リモートユーザーが内部のWebアプリケーションにアクセスするには、NetScaler Gateway Plug-inを使用する必要があります。

Citrix Receiver内でストアにアクセスするリモートユーザーに対してNetScaler Gatewayでの2要素認証を有効にする場合は、

NetScaler Gatewayで2つの認証ポリシーを作成する必要があります。プライマリの認証方法としてRADIUS（Remote Authentication Dial-In User Service）を構成し、セカンダリの認証方法としてLDAP（Lightweight Directory Access Protocol）を構成します。セッションプロファイルでセカンダリの認証方法が使用されるように資格情報インデックスを変更して、LDAP資格情報がStoreFrontに渡されるようにします。NetScaler Gatewayアプライアンスを StoreFront構成に追加する場合は、［ログオンの種類］を［ドメインおよびセキュリティトークン］に設定します。詳しくは、http://support.citrix.com/article/CTX125364を参照してください。

NetScaler GatewayからStoreFrontへの複数ドメイン認証を有効にするには、各ドメインのNetScaler Gateway LDAP認証ポリシーで［SSO Name Attribute］をuserPrincipalNameに設定します。使用されるLDAPポリシーが特定されるように、NetScaler Gatewayのログオンページでユーザーにドメインを指定させることができます。StoreFrontに接続できるようにNetScaler Gatewayセッションプロファイルを構成する場合は、シングルサインオンドメインを指定しないでください。管理者は、各ドメイン間の信頼関係を構成する必要があります。明示的に信頼されるドメインのみにアクセスを制限せず、ユーザーがどのドメインからもStoreFrontへログオンできるようにします。

NetScaler Gateway展開環境でサポートされる場合は、SmartAccess機能を使用して、XenDesktopおよびXenAppリソースへのユーザーアクセスをNetScaler Gatewayセッションポリシーに基づいて制御できます。SmartAccessについて詳しくは、「How SmartAccess works for XenApp and XenDesktop」を参照してください。

ユーザーはスマートカードとPINを使ってストアにアクセスします。StoreFrontをインストールする際、スマートカード認証はデフォルトで無効になっています。スマートカード認証は、Citrix Receiver、Citrix Receiver for Web、デスクトップアプライアンスサイト、およびXenApp Servicesサイトからストアに接続するユーザーに対して有効にすることができます。

スマートカード認証を使用すると、ユーザーのログオンプロセスを効率化して、同時にインフラストラクチャへのユーザーアクセスのセキュリティを強化できます。社内ネットワークへのアクセスは、公開キーのインフラストラクチャを使用した証明書ベースの2要素認証によって保護されます。秘密キーは、ハードウェアで保護されるため、スマートカードの外に漏れることはありません。ユーザーは、スマートカードとPINを使用してさまざまなコーポレートデバイスからデスクトップとアプリケーションにアクセスできるようになります。

スマートカードは、XenDesktopおよびXenAppで提供されるデスクトップとアプリケーションのユーザー認証をStoreFront経由で行うために使用できます。StoreFrontにスマートカードでログオンするユーザーは、App Controllerで提供されるアプリケーションにもアクセスできます。ただし、クライアント証明書認証を使用するApp Controller Webアプリケーションにアクセスするには、再度認証を受ける必要があります。

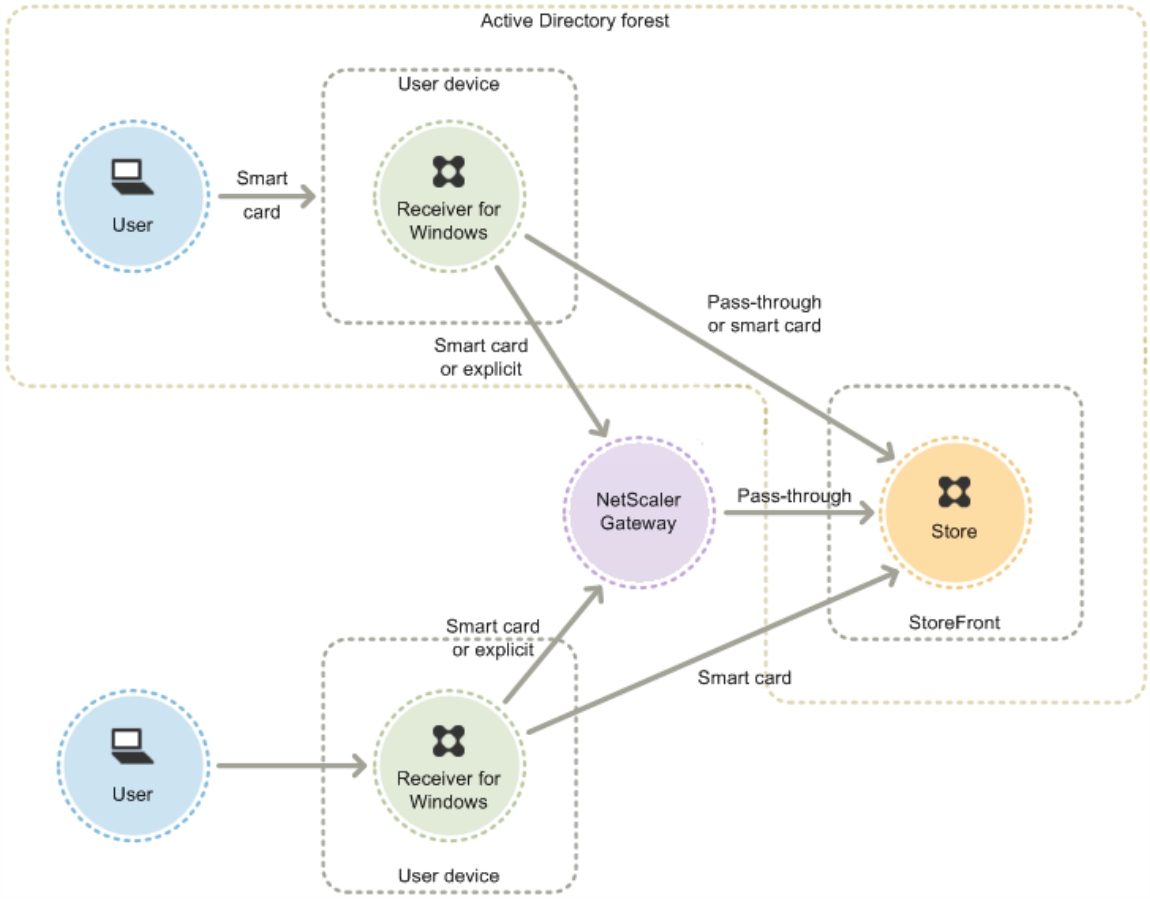
スマートカード認証を有効にする場合、StoreFrontサーバーが属しているMicrosoft Active Directoryドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにユーザーのアカウントが属している必要があります。双方向の信頼関係を含んでいるマルチフォレスト展開環境がサポートされます。

StoreFrontのスマートカード認証の構成は、ユーザーデバイス、インストールされているクライアント、およびデバイスがドメインに参加しているかどうかによって異なります。ドメインに参加しているデバイスとは、StoreFrontサーバーを含んでいるActive Directoryフォレスト内のドメインに属しているデバイスを意味します。

Citrix Receiver for Windowsでのスマートカードの使用

Citrix Receiver for Windowsを実行しているデバイスのユーザーは、スマートカードを使って直接またはNetScaler Gateway経由で認証を受けることができます。ドメイン参加デバイスとドメイン不参加デバイスの両方でスマートカード認証を使用できますが、ユーザーエクスペリエンスがわずかに異なります。

この図は、Citrix Receiver for Windowsを介したスマートカード認証を示しています。



ドメインに参加しているデバイスのローカルユーザーには、資格情報を再入力しなくて済むように、スマートカード認証を有効にします。ユーザーがスマートカードとPINを使ってデバイスにログオンしたら、それ以降PINを再入力する必要はありません。StoreFrontおよびデスクトップやアプリケーションにアクセスするときの認証は透過的に行われます。管理者は、Citrix Receiver for Windowsのパススルー認証を構成して、StoreFrontのドメインパススルー認証を有効にします。

ユーザーは、PINを使ってデバイスにログオンし、Citrix Receiver for Windowsの認証を受けます。アプリケーションおよびデスクトップを開始するときに、追加でPINの入力を求められることはありません。

ドメイン不参加デバイスのユーザーはCitrix Receiver for Windowsに直接ログオンするため、管理者は指定ユーザー認証へのフォールバックを有効にすることができます。管理者がスマートカード認証と指定ユーザー認証の両方を構成した場合、ユーザーは最初にスマートカードとPINを使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

ユーザーがNetScaler Gateway経由でデスクトップやアプリケーションにアクセスする場合は、スマートカードとPINを使って最低でも2回ログオン操作を行う必要があります。これはドメイン参加デバイスとドメイン不参加デバイスの両方に適用されます。ユーザーは、スマートカードとPINを使ってデバイスにログオンし、デスクトップやアプリケーションにアクセスするときにもう一度PINを入力します。管理者は、NetScaler Gateway認証のStoreFrontへのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。さらにNetScaler Gateway仮想サーバーを追加して、デスクトップやアプリケーションへのユーザー接続がそのNetScaler Gateway経由で行われるように構成します。ドメインに参加しているデバイスに対しては、Citrix Receiver for Windowsのパススルー認証も構成する必要があります。

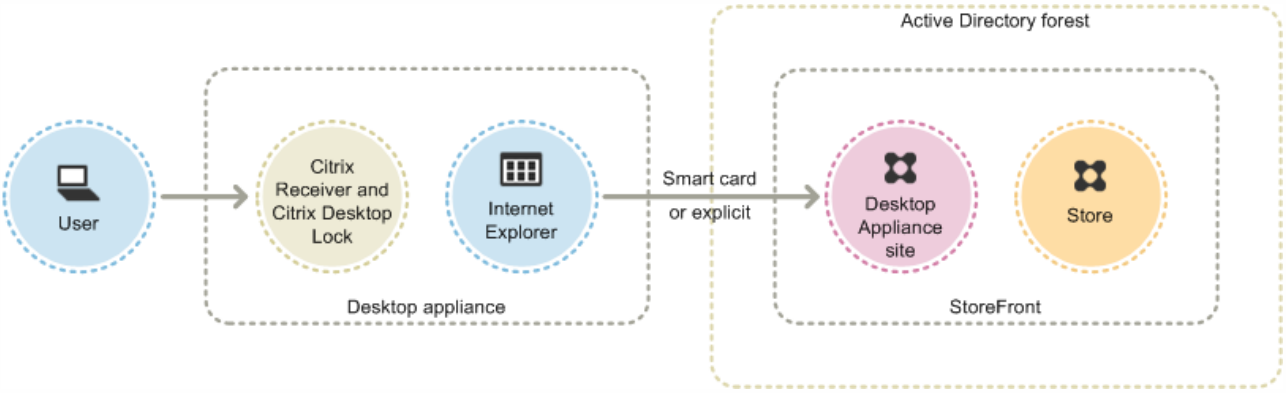
注:Citrix Receiver for Windows 4.2（最新バージョン）をお使いの場合、2つめのvServerをセットアップし、最適なゲートウェイルーティング機能を使用して、アプリケーションおよびデスクトップの開始時にPINの入力が不要となるようにすることができます。

ユーザーは、スマートカードとPINを使って、または指定ユーザーの資格情報を使ってNetScaler Gatewayにログオンできます。これにより、管理者はユーザーがNetScaler Gatewayにログオンするときに指定ユーザー認証へのフォールバックを有効にすることができます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gatewayに委任します。

デスクトップアプライアンスサイトでのスマートカードの使用

ドメイン不参加のWindowsデスクトップアプライアンスでは、ユーザーがスマートカードを使用してデスクトップにログオンできるように構成できます。アプライアンスにはCitrix Desktop Lockが必要で、デスクトップアプライアンスサイトへのアクセスにはInternet Explorerを使用する必要があります。

この図は、ドメイン不参加のデスクトップアプライアンスからのスマートカード認証を示しています。



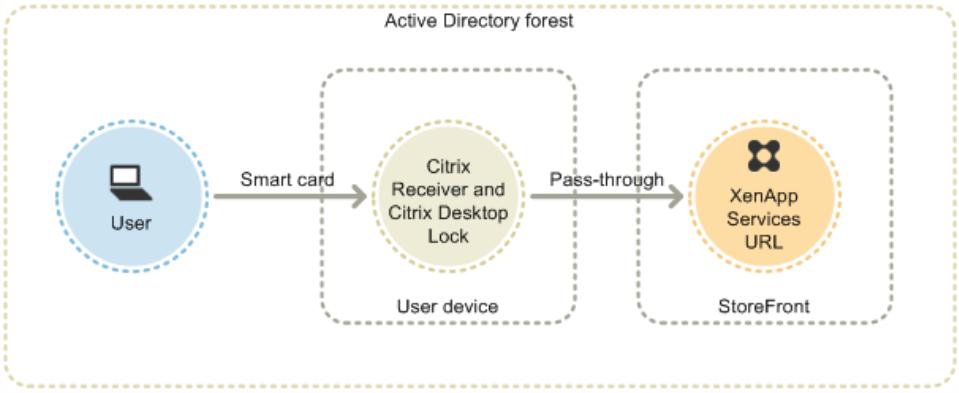
ユーザーがデスクトップアプライアンスにアクセスすると、Internet Explorerが全画面モードで起動し、デスクトップアプライアンスサイトのログオン画面が表示されます。ユーザーは、スマートカードとPINを使ってサイトの認証を受けます。デスクトップアプライアンスサイトでパススルー認証が構成されている場合、ユーザーはデスクトップやアプリケーションにアクセスするときに自動的に認証されます。PINの再入力は要求されません。パススルー認証が構成されていない場合は、デスクトップまたはアプリケーションにアクセスするときにPINをもう一度入力する必要があります。

管理者は、スマートカードでの認証に問題が生じた場合に指定ユーザー認証を使用できるように設定できます。これを行うには、デスクトップアプライアンスサイトにスマートカード認証と指定ユーザー認証の両方を構成します。この構成では、スマートカード認証がプライマリのアクセス方法とみなされます。そのため、ユーザーはまずPINの入力を要求されます。ただし、指定ユーザーの資格情報でログオンするためのリンクも表示されます。

XenApp Servicesサイトでのスマートカードの使用

ドメイン参加のデスクトップアプライアンスとCitrix Desktop Lockを実行している再目的化されたPCのユーザーは、スマートカードを使って認証を受けることができます。ほかのアクセス方法とは異なり、スマートカードのパススルー認証は、XenApp Servicesサイトでスマートカード資格情報が構成されている場合には自動的に有効になります。

この図は、Citrix Desktop Lockを実行しているドメイン参加のデバイスからのスマートカード認証を示しています。



ユーザーは、スマートカードとPINを使ってデバイスにログオンします。その後、Citrix Desktop Lockにより、ユーザーはXenApp Servicesサイトを介してサイレントにStoreFrontに認証されます。デスクトップやアプリケーションにアクセスするときは自動的に認証され、PINの再入力が要求されることはありません。

Citrix Receiver for Webでのスマートカードの使用

StoreFrontの管理コンソールを使用して、Citrix Receiver for Webでのスマートカード認証を有効にすることができます。

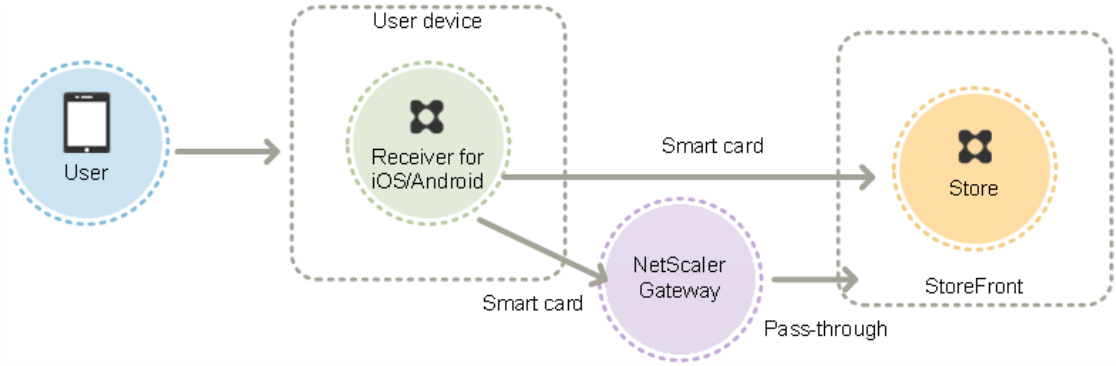
1. 左ペインで［Citrix Receiver for Web］ノードを選択します。
2. スマートカード認証を使用するサイトを選択します。
3. 右ペインで［認証方法の選択］を選択します。
4. ポップアップダイアログボックスでスマートカードのチェックボックスをオンにして、［OK］をクリックします。

ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用せずにストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用してストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

Citrix Receiver for iOSおよびAndroidでのスマートカードの使用

Citrix Receiver for iOSおよびCitrix Receiver for Androidを実行しているデバイスのユーザーは、スマートカードを使って直接またはNetScaler Gateway経由で認証を受けることができます。また、ドメインに参加していないデバイスを使用することもできます。



ローカルネットワーク上のデバイスの場合、ユーザーは最低でも2回ログオン操作を行う必要があります。ユーザーがStoreFrontで認証する場合、または初めてストアを作成する場合は、スマートカードPINの入力が求められます。さらに、ユーザーがデスクトップやアプリケーションにアクセスするときに、もう一度PINを入力します。この認証方法を構成するには、StoreFrontでスマートカード認証を有効にして、VDAにスマートカードドライバーをインストールします。

これらのCitrix Receiverに対しては、スマートカード認証またはドメイン資格情報による認証のいずれかを指定する必要があります。スマートカード認証を有効にしてストアを作成した後でドメイン資格情報による接続を許可するには、スマートカード認証が無効な別のストアを追加する必要があります。

ユーザーがNetScaler Gateway経由でデスクトップやアプリケーションにアクセスする場合は、スマートカードとPINを使って最低でも2回ログオン操作を行う必要があります。ユーザーは、スマートカードとPINを使ってデバイスにログオンし、デスクトップやアプリケーションにアクセスするときにもう一度PINを入力します。管理者は、NetScaler Gateway認証のStoreFrontへのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。さらにNetScaler Gateway仮想サーバーを追加して、デスクトップやアプリケーションへのユーザー接続がそのNetScaler Gateway経由で行われるように構成します。

ユーザーは、管理者が接続の認証をどう指定しているかに応じて、スマートカードとPIN、または指定ユーザー認証の資格情報を使用してNetScaler Gatewayにログオンできます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gatewayに委任します。認証方法を変更する場合は、接続を削除し、再作成する必要があります。

Citrix Receiver for Linuxでのスマートカードの使用

Citrix Receiver for Linuxを実行するデバイスを使用するユーザーは、ドメイン不参加のWindowsデバイスのユーザーと同様の方法で、スマートカードを使用して認証できます。ユーザーがスマートカードを使用してLinuxデバイスで認証されている場合にも、Citrix Receiver for Linuxには入力済みのPINを取得または再利用するメカニズムがありません。

Citrix Receiver for Windows用に構成したときと同じ方法で、サーバー側のコンポーネントのスマートカード認証を構成します。詳しくは、「How To Configure StoreFront 2.x and Smart Card Authentication for Internal Users using Stores」を参照してください。また、スマートカードの使用方法について詳しくは、docs.citrix.comの「Citrix Receiver for Linux」を参照してください。

ユーザーは最低でも1回のログオン操作を行う必要があります。ユーザーは、スマートカードとPINを使ってデバイスにログオンし、Citrix Receiver for Linuxの認証を受けます。ユーザーがデスクトップやアプリケーションにアクセスするときにPINを再入力する必要はありません。管理者は、StoreFrontのスマートカード認証を有効にします。

ユーザーはCitrix Receiver for Linuxに直接ログオンするので、管理者は指定ユーザー認証へのフォールバックを有効にすることができます。管理者がスマートカード認証と指定ユーザー認証の両方を構成した場合、ユーザーは最初にスマートカードとPINを使ったログオンを要求されますが、スマートカードでログオンできない場合は指定ユーザー認証を選択することができます。

ユーザーがNetScaler Gateway経由でデスクトップやアプリケーションにアクセスする場合は、スマートカードとPINを使って最低でも1回のログオン操作を行う必要があります。ユーザーは、スマートカードとPINを使ってデバイスにログオンします。デスクトップやアプリケーションにアクセスするときに、PINを再入力する必要はありません。管理者は、NetScaler Gateway認証のStoreFrontへのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。さらにNetScaler Gateway仮想サーバーを追加して、デスクトップやアプリケーションへのユーザー接続がそのNetScaler Gateway経由で行われるように構成します。

ユーザーは、スマートカードとPINを使って、または指定ユーザーの資格情報を使ってNetScaler Gatewayにログオンできます。これにより、管理者はユーザーがNetScaler Gatewayにログオンするときに指定ユーザー認証へのフォールバックを有効にすることができます。ユーザーがStoreFrontに透過的に認証されるように、NetScaler GatewayからStoreFrontへのパススルー認証を構成し、スマートカードユーザーの資格情報の検証をNetScaler Gatewayに委任します。

Citrix Receiver for LinuxでXenApp Servicesサポートサイトにアクセスする場合、スマートカードはサポートされません。

サーバーとCitrix Receiverの両方でスマートカードのサポートを有効にすると、スマートカード証明書のアプリケーションポリシーで許可されていれば、以下の目的でスマートカードを使用できます。

- スマートカードによるログオン認証。スマートカードを使って、Citrix XenAppサーバーやXenDesktopサーバーにログオンするユーザーを認証します。
- スマートカード対応アプリケーションのサポート。スマートカード対応の公開アプリケーションを使って、ローカルのスマートカードリーダーにアクセスできます。

XenApp Servicesサポートサイトでのスマートカードの使用

XenApp Servicesサポートサイトにログオンしてアプリケーションやデスクトップを開始するユーザーは、スマートカードを使って認証を受けることができます。特定のハードウェア、オペレーティングシステム、およびCitrix Receiverを使用する必要はありません。ユーザーがXenApp Servicesサポートサイトにアクセスしてスマートカードと PINを使ってログオンすると、PNAがユーザーIDを決定してStoreFrontでの認証を行い、使用できるリソースを返します。

パススルーおよびスマートカード認証が正しく動作するためには、[Citrix XML Serviceへの要求を信頼する] をオンにする必要があります。

Delivery Controller上でローカルの管理者アカウントを使用してWindows PowerShellを起動して、コマンドプロンプトで次のコマンドを実行します。これにより、StoreFrontから送信されたXML要求をDelivery Controllerが信頼するようになります。次の手順は、XenApp 7.5～7.8、およびXenDesktop 7.0～7.8に適用されます。

1. 「asnp Citrix*.」と入力してCitrixコマンドレットを読み込みます
2. **Add-PSSnapin citrix.broker.admin.v2**を実行します。
3. **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**を実行します。
4. PowerShellを閉じます。

XenApp Servicesサポートのスマートカード認証方法の構成について詳しくは、「XenApp Services URLの認証の構成」を参照してください。

重要な注意事項

StoreFrontでのユーザー認証にスマートカードを使用する場合は、次の要件と制限があります。

- スマートカード認証で仮想プライベートネットワーク（VPN）トンネルを使用するには、ユーザーがNetScaler Gateway Plug-inをインストールしてWebページ経由でログオンする必要があります。この場合、各手順でスマートカードとPINによる認証が必要になります。スマートカードユーザーは、NetScaler Gateway Plug-inを使用したStoreFrontへのパススルー

認証を使用できません。

- 同一ユーザーデバイス上で複数のスマートカードやスマートカードリーダーを使用することのできますが、スマートカードでのパススルー認証を有効にする場合は、ユーザーがデスクトップやアプリケーションにアクセスするときにスマートカードが1枚のみ挿入されていることを確認する必要があります。
- アプリケーション内でスマートカードを使用する場合（デジタル署名または暗号化機能など）、スマートカードの挿入またはPINの入力を求めるメッセージが表示されることがあります。これは、同時に複数のスマートカードが挿入されている場合に発生します。また、構成設定（通常グループポリシーを使用して構成されるPINキャッシュなどのミドルウェア設定）が原因で発生することもあります。スマートカードをリーダーに挿入しているにもかかわらずスマートカードの挿入を求めるメッセージが表示された場合は、［キャンセル］をクリックする必要があります。ただし、PINの入力が求められた場合は、PINを再入力する必要があります。
- ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用せずにストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- ドメイン参加デバイスを使用するCitrix Receiver for WindowsユーザーがNetScaler Gatewayを使用してストアにアクセスする場合、XenDesktopおよびXenAppへのスマートカードでのパススルー認証を有効にすると、その設定がストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- 各XenApp Servicesサイトに構成できる認証方法と各ストアで使用できるXenApp Servicesサイトは、それぞれ1つだけです。スマートカード認証に加えてほかの認証方法を有効にする必要がある場合は、認証方法ごとに個別のストアを作成し、それぞれのストアにXenApp Servicesサイトを1つずつ割り当てる必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
- StoreFrontインストール時のMicrosoftインターネットインフォメーションサービス（IIS）のデフォルト構成では、StoreFront認証サービスの証明書認証URLへのHTTPS接続でのみクライアント証明書が要求されます。それ以外のStoreFront URLにはクライアント証明書は必要ありません。この構成により、管理者は、スマートカードでの認証に問題が生じた場合に指定ユーザー認証を使用できるように設定できます。適用されるWindowsポリシー設定によっては、ユーザーが再認証なしにスマートカードを取り出すこともできます。

  すべてのStoreFront URLへのHTTPS接続でクライアント証明書が必要になるようにIISを構成する場合は、認証サービスとストアを同じサーバー上に配置する必要があります。この場合、すべてのストアに有効なクライアント証明書を使用する必要があります。このIISサイト構成では、スマートカードユーザーがNetScaler Gateway経由で接続できなくなり、指定ユーザー認証にもフォールバックされません。また、スマートカードをデバイスから取り出す場合は再度ログオンする必要があります。

ユーザーエクスペリエンスの最適化

May 22, 2017

StoreFrontには、ユーザーエクスペリエンスを向上させる機能があります。これらの機能は、新しいストアや、それに関連するCitrix Receiver for Webサイト、デスクトップアプライアンスサイト、およびXenApp Servicesサイトの作成時にデフォルトで構成されます。

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。ユーザーは、新しいデバイスにログオンするたびにすべてのアプリケーションを再起動する必要がなく、複数のデバイスを切り替えながら同じアプリケーションインスタンスを使用できます。これにより、たとえば病院で臨床医がワークステーションを切り替えて患者データにアクセスするときの時間を節約できます。

Citrix Receiver for Webサイト、およびXenApp Servicesサイト経由でストアに接続すると、ワークスペースコントロールがデフォルトで有効になります。ユーザーがログオンすると、実行したままのアプリケーションに自動的に再接続されます。たとえば、あるユーザーがCitrix Receiver for WebサイトまたはXenApp Servicesサイト経由でストアにログオンして、いくつかのアプリケーションを起動します。その後、ユーザーが別のデバイスで同じアクセス方法を使用して同じストアにログオンすると、実行中のアプリケーションが自動的に新しいデバイスで使用可能になります。ユーザーがストアで起動したすべてのアプリケーションは、そのストアからログオフすると自動的に切断されます。ただし、シャットダウンはされません。Citrix Receiver for Webサイトの場合は、同じWebブラウザーを使用してログオン、アプリケーションの起動、およびログオフを行う必要があります。

XenApp Servicesサイトでは、ワークスペースコントロールの構成を変更したり無効にしたりすることはできません。Citrix Receiver for Webサイトのワークスペースコントロールの構成について詳しくは、「ワークスペースコントロールの構成」を参照してください。

Citrix Receiver for Webサイトでワークスペースコントロールを使用する場合は、次の要件と制限があります。

- ホストされているデスクトップやアプリケーションからCitrix Receiver for Web サイトにアクセスする場合は、ワークスペースコントロールを使用できません。
- WindowsデバイスからCitrix Receiver for Webサイトにアクセスするユーザーについては、ユーザーデバイスにCitrix Receiverがインストールされていることをサイトで検出できる場合、およびCitrix Receiver for HTML5が使用される場合にのみ、ワークスペースコントロールが有効になります。
- 切断したアプリケーションに再接続するには、Internet ExplorerでCitrix Receiver for Webサイトにアクセスするユーザーは［ローカルイントラネット］または［信頼済みサイト］のゾーンにサイトを追加する必要があります。
- ただし、ワークスペースコントロールの設定にかかわらず、Citrix Receiver for Webサイトで使用可能なデスクトップが1つのみの場合、ユーザーのログオン時にそのデスクトップが自動的に起動するように構成すると、アプリケーションは再接続されません。
- アプリケーションを切断するときに、起動に使用したWebブラウザーを使用する必要があります。別のWebブラウザーで起動したリソースや、デスクトップや［スタート］メニューからCitrix Receiverで起動したリソースは、Receiver for Webサイトで切断したりシャットダウンしたりできません。

ユーザーが適切なアプリケーションをサブスクライブしてある場合、コンテンツリダイレクトにより、ユーザーデバイス上のローカルファイルがサブスクライブされたアプリケーションで開きます。このリダイレクトを有効にするには、XenDesktopまたはXenAppでアプリケーションを必要なファイルタイプと関連付けます。コンテンツリダイレクトは、新しいストアでデフォルトで有効になります。詳しくは、「ファイルタイプの関連付けを無効にするには」を参照してください。

管理者は、Microsoft Active Directoryドメインの資格情報でCitrix Receiver for Webサイトにログオンするユーザーがパスワードをいつでも変更できるように構成できます。または、パスワードの有効期限が切れたユーザーにのみパスワードの変更を許可することもできます。これにより、ユーザーがパスワードの失効によりデスクトップやアプリケーションにアクセスできなくなることを防ぐことができます。

Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。デフォルトでは、ユーザーに対する通知期間は、適用されるWindowsポリシーの設定によって決まります。パスワードの有効期限切れの警告は、内部ネットワークから接続しているユーザーにのみ表示されます。ユーザーによるパスワードの変更を有効にする方法について詳しくは、「認証サービスの構成」を参照してください。

デスクトップアプライアンスサイトにログオンするユーザーは、パスワードをいつでも変更できるようになっている場合でも、有効期限の切れたパスワードしか変更できません。デスクトップアプライアンスサイトにログオンした後では、パスワードを変更するためのオプションが提供されません。

認証サービスを作成したときのデフォルトの構成では、パスワードが失効しても、Citrix Receiver for Webサイトのユーザーはパスワードを変更できません。この機能を有効にする場合は、サーバーが属しているドメインのポリシーでユーザーによるパスワード変更が禁止されていないことを確認してください。ユーザーのパスワードを変更するには、StoreFrontはドメインコントローラーと通信する必要があります。

ユーザーによるパスワードの変更を有効にすると、この認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。

Citrix Receiver for Webサイトからデスクトップとアプリケーションの両方にアクセスできる場合、デフォルトでデスクトップとアプリケーションが別々のビューで表示されます。サイトにログオンすると、最初にデスクトップビューが表示されます。Citrix Receiver for Webサイトでユーザーがアクセスできるデスクトップが1つのみの場合、アクセス可能なアプリケーションがあるかどうかにかかわらず、ユーザーのログオン時にそのデスクトップが自動的に起動します。管理者は、Citrix Receiver for Webサイトに表示するビューを指定したり、デスクトップが自動的に起動するのを無効にしたりできます。詳しくは、「Configure how resources are displayed for users」を参照してください。

Citrix Receiver for Webサイトのビューの動作は、配信されるリソースの種類により異なります。たとえば、アプリケーションビューにアプリケーションが表示されるようにするには、ユーザーがそのアプリケーションをサブスクライブする必要があります。一方、ユーザーが使用できるすべてのデスクトップは自動でデスクトップビューに表示されます。このため、ユーザーはデスクトップビューからデスクトップを削除できず、デスクトップのアイコンをドラッグアンドドロップで並び替えることはできません。XenDesktop管理者がユーザーによるデスクトップの再起動を許可している場合は、デスクトップビューにデスクトップを再起動するためのコントロールが表示されます。単一のデスクトップグループの複数のデスクトップインスタンスがユーザーに提供される場合、Citrix Receiver for Webサイトではデスクトップ名に数字が追加されます。

Citrix ReceiverやXenApp Servicesサイトでストアに接続するユーザーの場合、デスクトップおよびアプリケーションの表示と動作は使用するCitrixクライアントにより異なります。

XenDesktopやXenAppでアプリケーションをユーザーに配信するときは、ストアのアプリケーションにアクセスするユーザーのエクスペリエンスを向上させるために、次のオプションについて検討します。アプリケーションの配信について詳しくは、

「デリバリーグループアプリケーションの作成」を参照してください。

- 使用できるリソースから必要なアプリケーションを簡単に見つけられるように、アプリケーションをフォルダー別に整理してユーザーに提供します。XenDesktopおよびXenAppでアプリケーションをフォルダーで管理すると、そのフォルダーがユーザーのCitrix Receiverでのアプリケーション一覧に反映されます。フォルダーを使用すると、アプリケーションの種類またはユーザーの役割に応じてアプリケーションをグループ化できます。
- アプリケーションを簡単に識別できるように、アプリケーションを配信するときにわかりやすい説明を入力します。この説明は、ユーザーのCitrix Receiverに表示されます。
- アプリケーションの説明として文字列KEYWORDS:Mandatoryを追加すると、そのアプリケーションはすべてのユーザーのCitrix Receiverのホーム画面に追加され、ユーザーがこれを削除できなくなります。ただし、ユーザーはホーム画面にほかのアプリケーションを追加したり、このキーワードが指定されていないアプリケーションをホーム画面から削除したりできます。
- アプリケーションを配信するときに説明としてKEYWORDS:Autoという文字列を追加すると、そのアプリケーションはストアのすべてのユーザーに自動的にサブスクライブされるようになります。この場合、ユーザーがストアにログオンすると、そのアプリケーションを手動でサブスクライブしなくても自動的にプロビジョニングされます。
- AppControllerで管理されるWebアプリケーションやSoftware-as-a-Service（SaaS）アプリケーションがストアのすべてのユーザーに自動的にサブスクライブされるようにするには、アプリケーション設定を構成するときに［App is available in Receiver to all users automatically］チェックボックスをオンにします。
- ユーザーが特定のXenDesktopアプリケーションに簡単にアクセスできるようにするために、そのアプリケーションをユーザーのCitrix Receiverの［おすすめ］一覧に表示できます。これを行うには、アプリケーションの説明として文字列KEYWORDS:Featuredを追加します。
  注：複数のキーワードを追加する場合は、KEYWORDS:Auto Featuredのようにスペースで区切ります。
- Citrix Receiver for Webサイトのデフォルトでは、XenDesktopおよびXenAppでホストされる共有デスクトップがほかの仮想デスクトップと同じように表示されます。この動作を変更するには、デスクトップの説明としてKEYWORDS:TreatAsAppという文字列を追加します。これにより、そのデスクトップはCitrix Receiver for Webサイトのデスクトップビューではなくアプリケーションビューに表示され、ユーザーはそのデスクトップをサブスクライブする必要があります。また、そのデスクトップはCitrix Receiver for Webサイトへのログオン時に自動起動せず、Desktop Viewerでアクセスできません。
- Windowsユーザーに対しては、ローカルにインストールされたアプリケーションのバージョンと、それに相当する配信されたインスタンスの両方が使用可能な場合に、ローカルにインストールされたアプリケーションが優先的に使用されるように指定できます。これを行うには、アプリケーションの説明として「KEYWORDS:prefer="application"」という文字列を追加します。ここでapplicationは、ショートカットファイル名として指定されたローカルアプリケーションの名前に含まれる単語、またはStart Menuフォルダーからローカルアプリケーションへの実行可能ファイル名を含む絶対パスです。このキーワードを持つアプリケーションをユーザーがサブスクライブすると、指定された名前またはパスがユーザーのデバイス上で検索され、アプリケーションがローカルにインストールされているかどうかが判断されます。アプリケーションが見つかった場合、ユーザーがアプリケーションをサブスクライブしてもショートカットは作成されません。この場合、サブスクライブしたアプリケーションをCitrix Receiverで起動すると、ローカルにインストールされたインスタンスが代わりに実行されます。詳しくは、「アプリケーション配信の構成」を参照してください。

StoreFrontの高可用性とマルチサイト構成

May 22, 2017

StoreFrontには、ストアにリソースを提供している展開環境間の負荷分散とフェールオーバーを有効にするための機能が多数用意されています。また、障害回復専用の展開環境を指定して回復性を高めることもできます。これらの機能を使用すると、StoreFrontの分散展開環境を構成してストアの高可用性を有効にできます。詳しくは、「可用性の高いマルチサイトストア構成のセットアップ」を参照してください。

StoreFrontのデフォルトでは、ストアにデスクトップとアプリケーションを配信するすべての展開環境が列挙され、そのすべてのリソースが個別に扱われます。このため、複数の展開環境から同じリソースが同じ名前で配信されていても、リソースごとにアイコンが表示されます。ストアの高可用性やマルチサイト構成を有効にすると、同じデスクトップまたはアプリケーションを配信するXenDesktopおよびXenAppの展開環境をグループ化して、それらのリソースを集約してユーザーに提供できます。グループ化された展開環境は同一である必要はありませんが、集約対象のリソースは、各サーバー上で名前とパスが同じである必要があります。

この機能により、すべてのXenDesktopおよびXenAppの展開環境で配信されているリソースがストアで集約され、ユーザーには1つのアイコンだけが表示されます。App Controllerアプリケーションは集約されません。ユーザーが集約リソースを起動すると、サーバーの可用性、そのユーザーがアクティブなセッションを確立済みかどうか、および管理者が指定した順番に基づいて、対象リソースから最適なインスタンスが選択されます。

StoreFrontでは、過負荷状態、または一時的に使用できない状態などで要求に応答できないサーバーが動的に監視されます。そのサーバーとの通信が再確立されるまで、別のサーバー上のリソースインスタンスがユーザーに提供されます。リソースの提供サーバーでサポートされている場合は、ユーザーが追加リソースを起動したときに、既存のユーザーセッションの再利用が試行されます。このため、ユーザーが選択した追加リソースが、そのユーザーの既存のセッションを実行している展開環境で提供されている場合、そのセッション内で追加リソースが起動します。これにより、各ユーザーのセッション数が最小限に抑えられるため、追加のデスクトップやアプリケーションの起動にかかる時間が短縮され、製品ライセンスをより効率的に使用できます。

サーバーの可用性と既存のユーザーセッションを確認した後、StoreFrontは指定された順番に基づいて、ユーザーが接続する展開環境を決定します。ユーザーが使用できる同等の展開環境が複数ある場合は、管理者の構成に基づいて、一覧の最初の展開環境または任意の展開環境が選択されます。一覧で最初に使用可能な展開環境が選択されるように構成すると、現在のユーザー数に対して使用中の展開環境の数を最小限に抑えることができます。一覧から展開環境がランダムに選択されるように構成すると、使用可能な展開環境間でユーザー接続を均一に分散させることができます。

XenDesktopおよびXenAppで配信されるリソースでは、一覧での展開環境の順序を無視して、ユーザーが特定の展開環境のデスクトップやアプリケーションに接続されるように設定できます。これにより、特定のデスクトップやアプリケーションでは専用の展開環境に優先的にユーザーが接続されるようにして、ほかのリソースでは別の展開環境に接続されるように構成できます。このように構成するには、優先する展開環境のデスクトップやアプリケーションの説明に「KEYWORDS:Primary」という文字列を追加し、別の展開環境のリソースに「KEYWORDS:Secondary」という文字列を追加します。この場合、管理者が指定した展開環境の順序にかかわらず、ユーザーは優先される展開環境（プライマリ）に接続されます。優先される展開環境が使用できない場合、セカンダリリソースを提供する展開環境に接続されます。

デフォルトでは、ストアにアクセスしているユーザーには、そのストア用に構成されているすべての展開環境から使用可能なすべてのリソースが集約されて表示されます。ユーザーごとに異なるリソースを提供するには、ストアやStoreFront展開環境を個別に構成できます。マルチサイト構成による高可用性をセットアップすると、Microsoft Active Directoryグループのユー

ザーメンバーシップに基づいて、特定の展開環境へのアクセスを提供することができます。これにより、単一のストアで、ユーザーグループごとに異なるエクスペリエンスを構成できます。

たとえば、すべてのユーザーに共通するリソースを1つの展開環境でグループ化し、別の展開環境では経理（Accounts）部門用に財務アプリケーションをグループ化します。このような構成では、Accountsユーザーグループに属していないユーザーは、このストアにアクセスしても共通リソースしか表示されません。Accountsユーザーグループのメンバーには、共通リソースと財務アプリケーションの両方が表示されます。

別の例として、より高速で強力なハードウェアを使用するパワーユーザー用の展開環境を作成して、ほかの展開環境と同じリソースを提供します。これにより、エグゼクティブチームなど、ビジネスクリティカルなユーザーのエクスペリエンスを向上させることができます。このストアにアクセスすると、すべてのユーザーに同じデスクトップやアプリケーションが表示されますが、Executivesユーザーグループのメンバーは、パワーユーザー用の展開環境のリソースに優先的に接続されます。

異なるStoreFront展開環境内の類似のストアから同じアプリケーションにユーザーがアクセスできるようにした場合、ユーザーのアプリケーションサブスクリプションをサーバーグループ間で同期する必要があります。サブスクリプションを同期しない場合、あるStoreFront展開環境のストアでアプリケーションをサブスクライブしたユーザーが別のストアにログオンしたときに、それらのアプリケーションをサブスクライブし直す必要があります。異なるStoreFront展開環境間を移動するユーザーにシームレスなエクスペリエンスを提供するため、異なるサーバーグループのストア間でユーザーのアプリケーションサブスクリプションが定期的に同期されるように構成できます。特定の間隔で同期したり、1日の特定の時刻に同期したりできます。詳しくは、「サブスクリプション同期の構成」を参照してください。

管理者は、障害回復専用の展開環境を構成できます。この展開環境は、ほかのすべての展開環境が使用できない場合にのみ使用されます。通常、障害回復用の展開環境はメインの展開環境とは異なる場所に配置し、メインの展開環境のリソースのサブセットだけを提供します。また、障害回復用の展開環境では必要以上に高いユーザーエクスペリエンスを提供しません。展開環境を障害回復用に使用することを指定した場合、その展開環境を負荷分散やフェールオーバーの対象から除外します。ほかのすべての展開環境が使用できなくならない限り、ユーザーは障害回復用の展開環境で提供されるデスクトップやアプリケーションにアクセスできません。

メインの展開環境での障害が解決した後では、ユーザーが障害回復用の展開環境のリソースを既に実行している場合でも、追加のリソースはメインの展開環境で起動します。この場合、障害回復用の展開環境で実行しているリソースから切断されることはありません。ただし、ユーザーがそのリソースを終了した後では、そのリソースを再度起動することはできなくなります。同様に、メインの展開環境での障害が解決した後では、障害回復用の展開環境の既存のセッションが再利用されることはありません。

同一ストアの複数の展開環境で個別のNetScaler Gatewayアプライアンスを構成している場合は、ユーザーが各展開環境にアクセスするための最適なアプライアンスを定義できます。たとえば、それぞれがNetScaler Gatewayアプライアンスを持つ、地理的に異なる2つの場所からリソースを集約するストアを作成する場合、一方の場所のNetScaler Gatewayを経由して接続しているユーザーは、もう一方の場所のデスクトップやアプリケーションを起動できます。ただし、デフォルトでは、ユーザーが最初に接続したアプライアンス経由でリソースが配信されるため、コーポレートWANを通過する必要があります。

ユーザーエクスペリエンスを向上させ、WANを経由するトラフィックを削減するため、展開環境ごとに「最適なNetScaler Gatewayアプライアンス」を指定できます。これにより、ユーザーがストアにアクセスするときに経由したアプライアンスにかかわらず、リソースを提供する展開環境のローカルのアプライアンスにユーザー接続が自動的にルーティングされます。

内部ネットワーク上のローカルユーザーをNetScaler Gatewayにログオンさせてエンドポイント解析を行う場合でも、最適な

NetScaler Gatewayアプライアンス機能を使用できます。この構成では、ユーザーはNetScaler Gatewayアプライアンスを経由してストアに接続しますが、ユーザーが内部ネットワーク上にいるため、リソースへの接続はNetScaler Gateway経由である必要はありません。この場合、最適なNetScaler Gatewayアプライアンスは有効にしますが、展開環境用のアプライアンスは指定しません。このため、デスクトップとアプリケーションへのユーザー接続はNetScaler Gateway経由ではなく、直接ルーティングされます。また、NetScaler Gatewayアプライアンスに特定の内部仮想サーバーIPアドレスを構成する必要がある点に注意してください。さらに、ローカルユーザーがアクセスできない内部ビーコンポイントを指定して、Citrix Receiverがネットワーク上の場所にかかわらずNetScaler Gateway経由でストアにアクセスするようにします。

StoreFrontでは、単一のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）を持つ複数のアプライアンスで構成される、広域サーバー負荷分散用のNetScaler Gateway展開環境がサポートされます。StoreFrontでユーザーを認証して適切なアプライアンスにユーザー接続をルーティングするためには、負荷分散構成の各アプライアンスを識別できる必要があります。アプライアンスのFQDNは広域サーバー負荷分散構成で一意の識別子として使用できないため、アプライアンスごとに一意のIPアドレスを使ってStoreFrontを構成する必要があります。通常、これはNetScaler Gateway仮想サーバーのIPアドレスになります。

負荷分散について詳しくは、「NetScalerによる負荷分散」を参照してください。

可用性の高いマルチサイトストアを構成するかどうかを決定する場合は、以下の要件と制限について考慮してください。

- デスクトップとアプリケーションは、集約対象の各サーバー上で名前とパスが同じである必要があります。さらに、それらのリソースのプロパティ（名前やアイコンなど）も同じであることが必要です。プロパティが異なる場合、Citrix Receiverが使用可能なリソースを列挙するときに、リソースプロパティの変更が発生することがあります。
- 割り当て済みのデスクトップ（事前割り当ておよび初回使用時割り当てのデスクトップ）は集約しないでください。このようなデスクトップのデリバリーグループに、集約対象のものと同じ名前およびパスが設定されていないことを確認してください。
- App Controllerアプリケーションは集約されません。
- 異なるStoreFront展開環境のストア間で、ユーザーのアプリケーションサブスクリプションを同期する場合は、各サーバーグループのストアに同じ名前を付ける必要があります。さらに、両方のサーバーグループは、ユーザーアカウントが属しているActive Directoryドメイン、またはそのドメインと信頼関係があるドメインのいずれかに属している必要があります。
- 同等展開環境グループ内のすべてのプライマリサイトが使用できない場合のみ、障害回復用のバックアップ展開環境へのアクセスが提供されます。複数の同等展開環境グループ間でバックアップ展開環境を共有する場合、各グループのすべてのプライマリサイトが使用できなくなったときにのみ障害回復リソースにアクセスできるようになります。

Install, set up, upgrade, and uninstall

May 25, 2017

To install and configure StoreFront, complete the following steps in order:

1. If you plan to use StoreFront to deliver XenDesktop and XenApp resources to users, ensure that the StoreFront server is joined to either the Microsoft Active Directory domain containing your users' accounts or a domain that has a trust relationship with the user accounts domain.

   Important:
   - For single server deployments you can install StoreFront on a non-domain-joined server.
   - StoreFront cannot be installed on a domain controller.

2. If not already present, StoreFront requires Microsoft .NET 4.5 Framework, which can be downloaded from Microsoft. You must have Microsoft .NET 4.5 installed before you can install StoreFront.
3. Optionally, if you plan to configure a multiple server StoreFront deployment, set up a load balancing environment for your StoreFront servers.

   To use NetScaler for load balancing, you define a virtual server to proxy your StoreFront servers. For more information on configuring NetScaler for load balancing, see Load balancing with NetScaler.

   1. Ensure that load balancing is enabled on your NetScaler appliance.
   2. For each StoreFront server, create individual HTTP or TLS load balancing services, as appropriate, using the StoreFront monitor type.
   3. Configure the services to insert the client IP address into the X-Forwarded-For HTTP header of requests forwarded to StoreFront, overriding any global policies.

      StoreFront requires users' IP addresses to establish connections to their resources.

   4. Create a virtual server and bind the services to the virtual server.
   5. On the virtual server, configure persistence using the cookie insert method if you have the latest Citrix Receivers installed on all platforms and you have no need to support Android; otherwise, configure persistence on the basis of source IP address. Ensure the Time To Live (TTL) is sufficient to enable users to stay logged on to the server as long as required.

      Persistence ensures that only the initial user connection is load balanced, after which subsequent requests from that user are directed to the same StoreFront server.

4. Optionally, enable the following features.

   - .NET Framework 4.5 Features > .NET Framework 4.5, ASP.NET 4.5

   Optionally, enable the following roles and their dependencies on the StoreFront server.

   - Web Server (IIS) > Web Server > Common HTTP Features > Default Document, HTTP Errors, Static Content, HTTP Redirection
   - Web Server (IIS) > Web Server > Health and Diagnostics > HTTP Logging
   - Web Server (IIS) > Web Server > Security > Request Filtering, Windows Authentication

- On Windows Server 2012 servers:

  Web Server (IIS) > Web Server > Application Development > .NET Extensibility 4.5, Application Initialization, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters

  On Windows Server 2008 R2 servers:

  Web Server (IIS) > Web Server > Application Development > .NET Extensibility, Application Initialization, ASP.NET, ISAPI Extensions, ISAPI Filters

- Web Server (IIS) > Management Tools > IIS Management Console, IIS Management Scripts and Tools

The StoreFront installer checks that all the features and server roles above are enabled.

5. Install StoreFront.

   If you intend the server to be part of a server group, both the StoreFront installation location and IIS website settings, physical path and site IDs must be consistent across them.
6. Optionally, configure Microsoft Internet Information Services (IIS) for HTTPS if you plan to use HTTPS to secure communications between StoreFront and users' devices.

   HTTPS is required for smart card authentication. By default, Citrix Receiver requires HTTPS connections to stores. You can change from HTTP to HTTPS at any time after installing StoreFront, provided the appropriate IIS configuration is in place.

   To configure IIS for HTTPS, use the Internet Information Services (IIS) Manager console on the StoreFront server to create a server certificate signed by your domain certification authority. Then, add HTTPS binding to the default website. For more information about creating a server certificate in IIS, see http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate. For more information about adding HTTPS binding to an IIS site, see http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding.
7. Ensure your firewalls and other network devices permit access to TCP port 80 or 443, as appropriate, from both inside and outside the corporate network. In addition, ensure that any firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.

   When you install StoreFront, a Windows Firewall rule is configured enabling access to the StoreFront executable through a TCP port randomly selected from all unreserved ports. This port is used for communications between the StoreFront servers in a server group.
8. If you plan to use multiple Internet Information Services (IIS) websites, after creating the websites in IIS, use the PowerShell SDK to create a StoreFront deployment in each of those IIS websites. For more information, see Multiple Internet Information Services (IIS) websites.
   Note: StoreFront disables the management console when it detects multiple sites and displays a message to that effect.
9. Use the Citrix StoreFront management console to configure your server.

Important

To avoid potential errors and data loss when installing StoreFront, ensure all applications are closed and no other tasks or operations are running on the target system.

1. Download the installer from the download page.
2. Log on to the StoreFront server using an account with local administrator permissions.
3. Ensure that the required Microsoft .NET 4.5 Framework is installed on the server.
4. Browse the download package, locate CitrixStoreFront-x64.exe, and run the file as an administrator.
   Note: On Windows Server 2008 R2 servers, a message may be displayed indicating that the .NET feature will be enabled. If this message appears, click Yes.
5. Read and accept the license agreement, and click Next.
6. If the Review prerequisites page appears, click Next.
7. On the Ready to install page, check the prerequisites and StoreFront components that are listed for installation and click Install.
   Before the components are installed, the following roles are enabled if they are not already configured on the server.

   - Web Server (IIS) > Web Server > Common HTTP Features > Default Document, HTTP Errors, Static Content, HTTP Redirection
   - Web Server (IIS) > Web Server > Health and Diagnostics > HTTP Logging
   - Web Server (IIS) > Web Server > Security > Request Filtering, Windows Authentication
   - On Windows Server 2012 servers:

     Web Server (IIS) > Web Server > Application Development > .NET Extensibility 4.5, Application Initialization, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters

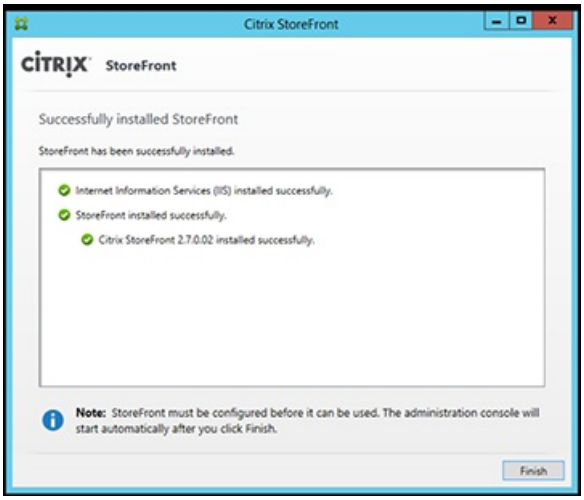
     On Windows Server 2008 R2 servers:

     Web Server (IIS) > Web Server > Application Development > .NET Extensibility, Application Initialization, ASP.NET, ISAPI Extensions, ISAPI Filters

   - Web Server (IIS) > Management Tools > IIS Management Console, IIS Management Scripts and Tools

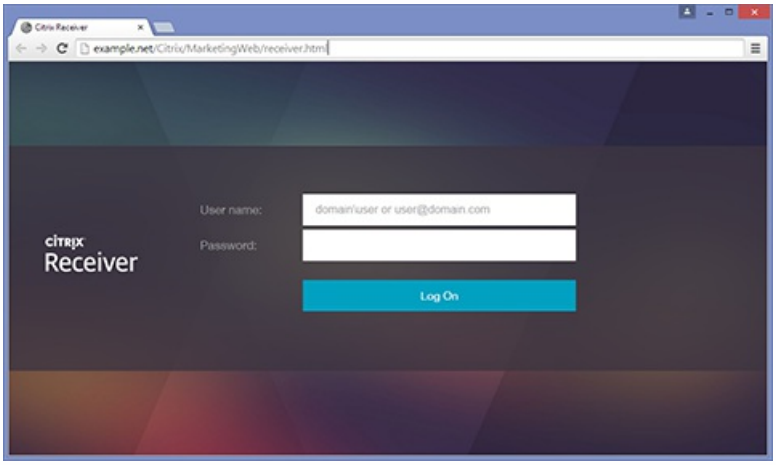
   The following features are also enabled if they are not already configured.

   - .NET Framework 4.5 Features > .NET Framework 4.5, ASP.NET 4.5
8. When the installation is complete, click Finish. The Citrix StoreFront management console starts automatically. You can also open StoreFront from the Start screen.



9. In the Citrix Storefront management console, click Create a new deployment.
    1. Specify the URL of the StoreFront server in the **Base URL** box.
    2. On the **Store Name** page, specify a name for your store, and click Next.
10. On the **Delivery Controllers** page, list the infrastructure – the details of the XenApp or XenDesktop services - that is providing the resources you want to make available in the store. You can enter a "dummy" server here; however, no apps will display in the store.
11. Set the **Transport type** and the **Port**. You can specify HTTP and port 443 and click **OK**. Alternatively, copy settings from an existing Web Interface or StoreFront deployment.
12. On the **Remote Access** page, select None. If you are using NetScaler Gateway, select No VPN Tunnel and enter your gateway details.
13. On the **Remote Access** page, select Create. Once the store has been created, click Finish.

Your store is now available for users to access through the Citrix Receiver for Web site, which enables users to access their desktops and apps through a webpage.
The URL for users to access the Citrix Receiver for Web site for the new store is displayed. For example: example.net/Citrix/MarketingWeb/. Log on and you will access the new user interface in Citrix Receiver.



If you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous statistics and usage information are sent to Citrix to improve the quality and performance of Citrix products.

By default, you are automatically enrolled in CEIP when you install StoreFront. The first upload of data occurs approximately seven days after you install StoreFront. You can change this default in a registry setting. If you change the registry setting before installing StoreFront, that value will be used. If you change the registry setting before upgrading StoreFront, that value will be used.

> **警告**
>
> Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Registry setting that controls automatic upload of analytics (default = 1):

Location: HKLM:\Software\Citrix\Telemetry\CEIP

Name: Enabled

Type: REG_DWORD

Value: 0 = disabled, 1 = enabled

By default, the "Enabled" property is hidden in the registry. When it remains unspecified, the automatic upload feature is enabled.

Using PowerShell, the following cmdlet disables enrollment in CEIP:

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

Note: The registry setting controls the automatic upload of anonymous statistics and usage information for all components on the same server. For example, if you have installed StoreFront on the same server as the Delivery Controller and decide to opt out of CEIP using the registry setting, the opt out will apply to both components.

CEIP data collected from StoreFront

The following table gives examples of the type of anonymous information collected. The data does not contain any details that identify you as a customer.

Data	Description
StoreFront version	String denoting the installed version of Storefront. For example, "3.8.0.0"
Stores count	A counter for the number of Stores in the deployment.
Server Count in server group	A counter for the number of Servers in the Server group.
Delivery Controller Count per store	List of numeric values indicating the number of Delivery Controllers available for each Store in the Deployment.
HTTPS enabled	String denoting whether https is enabled for the deployment. "True" or "False".
Classic experience enabled for Citrix Receiver	List of Booleans denoting whether "Classic Experience" is enabled for each Web Receiver. TRUE or FALSE for each Web Receiver.
HTML5 setting for Citrix Receiver	List of Strings denoting the HTML5 Receiver setting for each Web Receiver. "Always","Fallback","Off" for each Web Receiver.
Workspace control enabled for Citrix Receiver	List of Booleans denoting whether "Workspace Control" is enabled for each Web Receiver. TRUE or FALSE for each Web Receiver.

Remote Access enabled for store	List of Strings denoting whether "Remote Access" is enabled for each Store in the Deployment. "ENABLED" or "DISABLED" for each store.
Gateways count	A counter for the number of NetScaler Gateways configured in the deployment.

To install StoreFront at a command prompt

1. Log on to the StoreFront server using an account with local administrator permissions.
2. Ensure that all of the requirements for installation of StoreFront are met before installing StoreFront. Refer to Before installing and configuring for details.
3. Browse your installation media or download package, locate CitrixStoreFront-x64.exe, and copy the file to a temporary location on the server.
4. At a command prompt, navigate to the folder containing the installation file and type the following command.

   CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation]
   [-WINDOWS_CLIENT filelocation\filename.exe]
   [-MAC_CLIENT filelocation\filename.dmg]

   Use the -silent argument to perform a silent installation of StoreFront and all the prerequisites. By default, StoreFront is installed at C:\Program Files\Citrix\Receiver StoreFront\. However, you can specify a different installation location using the -INSTALLDIR argument, where installationlocation is the directory in which to install StoreFront. Note that if you intend the server to be part of a server group, both the StoreFront installation location and IIS website settings, physical path and site IDs must be consistent across them.

   By default, if a Citrix Receiver for Web site cannot detect Citrix Receiver on a Windows or Mac OS X device, the user is prompted to download and install the appropriate Citrix Receiver for their platform from the Citrix website. You can modify this behavior so that users download the Citrix Receiver installation files from the StoreFront server instead. For more information, see Make Citrix Receiver installation files available on the server.

   If you plan to make this configuration change, specify the -WINDOWS_CLIENT and -MAC_CLIENT arguments to copy Citrix Receiver for Windows and Citrix Receiver for Mac installation files, respectively, to the appropriate location in your StoreFront deployment. Replace filelocation with the directory containing the installation file that you want to copy and filename with the name of the Citrix Receiver installation file. Citrix Receiver for Windows and Citrix Receiver for Mac installation files are included on your StoreFront installation media or download package.

To upgrade existing StoreFront 2.0 through 3.0.x deployments to this version of StoreFront, run the installation file for this version of StoreFront. Releases before StoreFront 2.0 cannot be upgraded directly. Instead, you must first upgrade StoreFront 1.2 to StoreFront 2.0 before upgrading to this StoreFront. Similarly, you cannot upgrade Storefront 1.1 to this StoreFront directly. You must upgrade Storefront 1.1 to StoreFront 1.2 and then again to StoreFront 2.0 before finally upgrading to this StoreFront.

Once the upgrade process is started, it cannot be rolled back. If the upgrade is interrupted or cannot be completed, the existing configuration is removed but StoreFront is not installed. Before starting to upgrade, you must disconnect users from the StoreFront deployment and prevent users from accessing the servers while the upgrade is in progress. This ensures that all StoreFront files are accessible by the installer during the upgrade. If any files cannot be accessed by the installer, they cannot be replaced and so the upgrade will fail, resulting in the removal of the existing StoreFront configuration. StoreFront does not support multiple server deployments containing different product versions, so all servers in a group

must be updated to the upgraded version before granting access to the deployment. Concurrent upgrade is not supported for multiple server deployments, servers must be upgraded sequentially. Citrix recommends that you back up your data before upgrading.

Uninstalling StoreFront removes the authentication service, stores, users' application subscriptions, Citrix Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs. This means that if you decide to uninstall StoreFront, you must manually recreate your services, stores, and sites when you reinstall StoreFront. Upgrading also enables you to preserve your StoreFront configuration and leaves users' application subscription data intact so that users do not need to resubscribe to all of their applications.

Upgrading the operating system version on a server running StoreFront is not supported. Citrix recommends that you install StoreFront on a new installation of the operating system.

Important

Before you start the upgrade:

- Close all other applications on the StoreFront server.
- Close all command line and PowerShell windows.

To upgrade existing StoreFront 2.0 through 3.0.x to this version of StoreFront

1. Disable access to the deployment through the load balancing environment. Disabling the load balancing URL prevents users from connecting to the deployment during the upgrade process.
2. Back up all the servers in the server group.
3. Remove one of the servers from the existing server group.
4. Restart the server you removed.
   Note that you can use a parallel load balancer to check the new server group as you build it. The variant that maximizes availability and further minimizes risk involves removing and upgrading only one server from the original server group. You can then build the new group out of new machines rather than machines taken out of the original server group.
5. Upgrade the server you removed using an admin account with no other installations running and a minimum of other applications.
6. Check that the server you removed has upgraded successfully.
7. Remove another one of the servers in the existing server group from the load balancer.
8. Restart the server you removed for the same reasons noted in Step 1.
9. Uninstall the currently installed version of StoreFront and install the new version of StoreFront.
10. Join the newly installed server into a new server group consisting of all the upgraded servers and the freshly installed servers, and check they are functioning correctly.
11. Repeat Steps 3-10 until the new server group has sufficient capacity to take over from the old server group, point the load balancer at the new server group, and check that it is functioning correctly.
12. Repeat Steps 3-10 for the remaining servers, adding each one to the load balancer after each successful upgrade.

ヒント

- If you want to maximize availability, you can maintain access to the original server group during the upgrade process until the new server group becomes available. To do this;
  1. Skip Step 1.

2. Modify Step 11 to include disabling access to the original server group using the load balancer. Export subscription data from the original server group and import it into the new server group. Enable access to the new server group using the load balancer.

   This ensures that any subscription changes made by users after Step 3 and before Step 11 are available in the new server group.

- You can further maximize availability by removing only one server from the original server group and upgrading it, and then building the new server group using new servers rather than servers removed from the original server group. When the new server group is in production, you can retire the old servers.

When the Citrix StoreFront management console first starts, two options are available.

- Create a new deployment. Configure the first server in a new StoreFront deployment. Single-server deployments are ideal for evaluating StoreFront or for small production deployments. Once you have configured your first StoreFront server, you can add more servers to the group at any time to increase the capacity of your deployment.
- Join existing server group. Add another server to an existing StoreFront deployment. Select this option to rapidly increase the capacity of your StoreFront deployment. External load balancing is required for multiple server deployments. To add a new server, you will need access to an existing server in the deployment.

In addition to the product itself, uninstalling StoreFront removes the authentication service, stores, Citrix Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs, and their associated configurations. The subscription store service containing users' application subscription data is also deleted. In single-server deployments, this means that details of users' application subscriptions are lost. However, in multiple server deployments these data are retained on other servers in the group. Prerequisites enabled by the StoreFront installer, such as the .NET Framework features and the Web Server (IIS) role services, are not removed from the server when StoreFront is uninstalled.

1. Log on to the StoreFront server using an account with local administrator permissions.
2. On the Windows **Start** screen or Apps screen, locate the **Citrix StoreFront** tile. Right-click the tile and click **Uninstall**.
3. In the **Programs and Features** dialog box, select **Citrix StoreFront** and click **Uninstall** to remove all StoreFront components from the server.
4. In the **Uninstall Citrix StoreFront** dialog box, click **Yes**. When the uninstallation is complete, click **OK**.

新しい展開環境の作成

May 22, 2017

1. 新しいサーバー上でCitrix StoreFront管理コンソールを開きます。これを行うには、Windowsの[スタート]画面または［アプリ］画面で［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの結果ペインで、［新しい展開環境の作成］をクリックします。
3. ［ベースURL］ボックスで、StoreFrontサーバーまたは負荷分散環境（複数サーバーの展開環境の場合）のURLを指定します。
   負荷分散環境をセットアップしていない場合は、サーバーのURLを入力します。展開環境のベースURLはいつでも変更できます。

   Microsoftインターネットインフォメーションサービス（IIS）でHTTPSが正しく構成されている場合は、StoreFront管理コンソールの［ベースURLの変更］タスクでHTTPをHTTPSに変更することもできます。

4. ［次へ］を選択して、認証サービスをセットアップします。このサービスは、ユーザーをMicrosoft Active Directoryで認証します。
   StoreFrontとユーザーデバイス間の通信をHTTPSで保護するには、Microsoftインターネットインフォメーションサービス（IIS）でHTTPSを構成する必要があります。IISでHTTPSが構成されていない場合、StoreFrontの通信にHTTPが使用されます。

   デフォルトでは、Citrix Receiverはストアへの接続にHTTPSを必要とします。StoreFrontがHTTPS用に構成されていない場合、Citrix ReceiverでHTTP接続が使用されるようにユーザーが構成を変更する必要があります。スマートカード認証を使用する場合はHTTPSが必要です。IISでHTTPSが適切に構成されている場合は、StoreFrontの構成後に必要に応じていつでもHTTPをHTTPSに変更できます。詳しくは、「サーバーグループの構成」を参照してください。

   Microsoftインターネットインフォメーションサービス（IIS）でHTTPSが正しく構成されている場合は、StoreFront管理コンソールの**［ベースURLの変更］**タスクでHTTPをHTTPSに変更することもできます。

5. ［ストア名］ページで、ストアの名前を指定して、非認証（匿名）ユーザーのみにストアへのアクセスを許可するかしないかを指定し、［次へ］をクリックします。
   StoreFrontストアでは、ユーザーに提供するデスクトップとアプリケーションが集約されます。ストアの名前はCitrix Receiverでユーザーアカウントの下に表示されるため、ユーザーにとってわかりやすい名前を指定してください。

6. ［Controller］ページでは、リソースを提供するインフラストラクチャを一覧に追加します。ストアにデスクトップとアプリケーションを追加するには、以下の適切な手順に従います。XenDesktop、XenApp、およびXenMobile（App Controller）の展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順を繰り返し、ストアにリソースを提供するすべての展開環境を追加します。
   - XenDesktopおよびXenAppのリソースのストアへの追加
   - App Controllerアプリケーションのストアへの追加
7. 必要なリソースをすべてストアに追加したら、［Controller］ページの［次へ］をクリックします。
8. ［リモートアクセス］ページでは、公共のネットワーク上のユーザーに内部リソースへのアクセス（リモートアクセス）を提供するかどうか、およびその方法を指定します。
   - 公共のネットワーク上でストアをユーザーが使用できるようにするには、**［リモートアクセスの有効化］**チェックボックスをオンにします。このチェックボックスをオフにすると、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
   - NetScaler Gateway経由でアクセスするユーザーにストアのリソースのみを提供するには、**［StoreFrontを介して配信されたリソースへのアクセスのみをユーザーに許可する（VPNトンネルなし）］**を選択します。
   - SSL（Secure Sockets Layer）仮想プライベートネットワーク（Virtual Private Network：VPN）トンネルを介して内部

ネットワーク上のストアおよびそのほかのすべてのリソースへのアクセスを提供するには、**[内部ネットワーク上のすべてのリソースへのアクセスをユーザーに許可する（完全VPNトンネル）]**を選択します。この場合、ユーザーはVPNトンネルを確立するためのNetScaler Gateway Plug-inを使用する必要があることがあります。

NetScaler Gatewayを経由するストアへのリモートアクセスを有効にすると、認証方法としてNetScaler Gatewayからのパススルーが自動的に有効になります。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。

9. リモートアクセスを有効にした場合は、ユーザーがストアにアクセスするときに使用するNetScaler Gateway展開環境を一覧に追加します。NetScaler Gateway展開環境を追加するには、以下の適切な手順に従います。必要に応じて手順を繰り返し、新しい展開環境を追加します。
   - NetScaler Gatewayアプライアンスを介したストアへのリモートアクセスを有効にする
   - Access Gateway 5.0クラスターを介したストアへのリモートアクセスを有効にする
10. NetScaler Gatewayの展開環境をすべて追加したら、［NetScaler Gatewayアプライアンス］の一覧で、ユーザーがストアへのアクセスに使用する展開環境を選択します。複数のゲートウェイ環境を介したアクセスを有効にする場合は、デフォルトで使用されるアプライアンスを指定します。［次へ］をクリックします。
11. **[認証方法]**ページで、ユーザーがストアへの認証に使用する方法を選択し、**[次へ]**をクリックします。次の方法から選択できます。

- **ユーザー名とパスワード**：ユーザーは、ストアにアクセスするときに、資格情報を入力すると認証されます。
- **SAML認証**：ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。
- **ドメインパススルー**：ユーザーはドメインに参加しているWindowsコンピューターにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。
- **スマートカード**：ユーザーはスマートカードとPINを使ってストアにアクセスします。
- **HTTP基本認証**：ユーザー認証は、StoreFrontサーバーのIIS Webサーバーで実行されます。
- **NetScaler Gatewayを介したパススルー**：ストアにアクセスする場合、NetScaler Gatewayへの認証を実行して自動的にログオンされます。リモートアクセスが有効になるとこれは自動的にチェックされます。

12. **[XenApp Services URL]**ページで、Program Neighborhood Agentを使ってアプリケーションおよびデスクトップにアクセスするユーザーのXenApp Service URLを構成します。

13. ストアを作成した後は、Citrix StoreFront管理コンソールでさらに多くのオプションを使用できるようになります。詳しくは、さまざまな管理アーティクルを参照してください。

ストアが作成されました。ただし、Citrix Receiver側でもストアに接続するための詳細を構成する必要があります。ユーザーによるReceiverの構成プロセスを簡単にするために、いくつかの方法が用意されています。詳しくは、「ユーザーアクセスオプション」を参照してください。

また、Citrix Receiver for Webサイトを使用すると、ユーザーがWebページからデスクトップやアプリケーションにアクセスできるようになります。新しいストアにアクセスするためのCitrix Receiver for WebサイトのURLは、ストアを作成するときに表示されます。

デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。ドメインに参加していないデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトから直接そのストアに接続できます。XenApp Services URLの形式は、http[s]://serveraddress/Citrix/storename/PNAgent/config.xmlの形式です。ここで、serveraddressはStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、storenameは上記手順5で指定した名前です。

StoreFrontの追加のインスタンスをインストールするときに既存のサーバーグループにサーバーを追加するオプションを選択

することで、展開環境に複数のサーバーをすばやく追加できます。

XenAppおよびXenDesktopで提供されるデスクトップやアプリケーションを、StoreFrontサーバーの初回構成時に作成されるストアで使用できるようにするには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1.～6.を完了しておいてください。

1. StoreFrontコンソールの［Controller］ページで、［追加］をクリックします。
2. ［Controllerの追加］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、リソースを提供するインフラストラクチャの種類（［XenDesktop］、［XenApp］、または［XenMobile］）を選択します。
3. サーバーの名前またはIPアドレスを［サーバー］の一覧に追加します。この一覧に複数のサーバーを追加すると、その順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。
4. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。
   - XenAppサーバーとの通信でSSL Relayによるホスト認証とデータの暗号化を実行するには、［SSL Relay］を選択します。

   注：StoreFrontとサーバーの間の通信でHTTPSまたはSSL Relayを使用する場合は、［サーバー］ボックスの一覧に指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。
5. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続およびSSL Relay接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用されるポート番号を指定する必要があります。
6. StoreFrontとXenAppサーバーの間の接続をSSL Relayで保護する場合は、SSL RelayのTCPポートを［SSL Relayポート］ボックスで指定します。デフォルトのTCPポートは443です。SSL Relayを実行するすべてのサーバーで同じポートが構成されていることを確認してください。

XenDesktop、XenApp、およびXenMobileの展開環境を自由に組み合わせてストアを作成できます。XenDesktopサイトまたはXenAppファームをさらに追加する場合は、上記手順を繰り返します。App Controllerで管理されるアプリケーションをストアで使用できるようにするには、「App Controllerアプリケーションのストアへの追加」の手順に従います。必要なリソースをすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順7.以降に従います。

App Controllerで管理されるアプリケーションを、StoreFrontサーバーの初回構成時に作成されるストアで使用できるようにするには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1.～6.を完了しておいてください。

1. ［ストアの作成］ウィザードの［Delivery Controller］ページで、［追加］をクリックします。
2. ［Delivery Controllerの追加］ダイアログボックスで、追加するApp Controller仮想アプライアンスに対するわかりやすい名前を指定します。名前にスペースが含まれないようにしてください。［AppController］を選択します。
3. App Controller仮想アプライアンスの名前またはIPアドレスを［サーバー］ボックスに入力し、App Controllerへの接続に使用するStoreFrontのポートを指定します。デフォルトのTCPポートは443です。

XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。ほかのApp Controlle

仮想アプライアンスで管理されるアプリケーションをストアに追加するには、上記の手順を繰り返します。XenDesktopおよびXenAppで提供されるデスクトップやアプリケーションをストアで使用できるようにするには、「XenDesktopおよびXenAppのリソースのストアへの追加」の手順に従います。必要なリソースをすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順7.以降に従います。

StoreFrontサーバーの初回構成時に作成されるストアへの、NetScaler Gatewayアプライアンスを介したリモートアクセスを構成するには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1.～6.を完了しておいてください。

1. StoreFrontコンソールの［リモートアクセス］ページで、［追加］をクリックします。
2. ［NetScaler Gatewayアプライアンスの追加］ダイアログボックスで、NetScaler Gatewayアプライアンスにわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

3. アプライアンスの仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   ストアに内部および外部アクセスするための単一の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）の作成について詳しくは、「ストアに内部および外部アクセスするための単一のFQDNの作成」を参照してください。

4. スタンドアロンAccess Gateway 5.0アプライアンスを追加する場合は、［展開モード］の一覧で［アプライアンス］を選択します。それ以外の場合は、必要に応じてNetScaler GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
   このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

5. NetScaler Gateway 10.1、Access Gateway 10、またはAccess Gateway 9.3のアプライアンスを追加する場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
   - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
   - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
   - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

   スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。

6. ［コールバックURL］ボックスに、NetScaler Gateway認証サービスのURLを入力します。URLの標準的な部分は自動的に補完されます。［Next］をクリックします。
   アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

7. XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、[Secure Ticket Authority（STA）] ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
   STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

8. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
   ［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

9. ［作成］をクリックします。これにより、［リモートアクセス］ページの一覧にNetScaler Gatewayの展開環境が追加されます。

展開環境をさらに追加する場合は、上記手順を繰り返します。Access Gateway 5.0クラスターを介したリモートアクセスを構成するには、「Access Gateway 5.0クラスターを介したストアへのリモートアクセスを有効にする」の手順に従います。NetScaler Gatewayの展開環境をすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順10.以降に従います。

StoreFrontサーバーの初回構成時に作成されるストアへの、Access Gateway 5.0クラスターを介したリモートアクセスを構成するには、次の手順に従います。このトピック冒頭の「新しい展開環境の作成」の手順1.～6.を完了しておいてください。

1. StoreFrontコンソールの［リモートアクセス］ページで、［追加］をクリックします。
2. ［NetScaler Gatewayアプライアンスの追加］ダイアログボックスで、クラスターにわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

3. クラスターのユーザーログオンポイントのURLを入力して、［バージョン］の一覧で［5.x］を選択します。
4. ［展開モード］の一覧で［Access Controller］を選択して、［次へ］をクリックします。
5. ［アプライアンス］ページで、クラスター内のアプライアンスのIPアドレスまたはFQDN（Fully Qualified Domain Names：完全修飾ドメイン名）を一覧に追加して、［次へ］をクリックします。
6. ［サイレント認証を有効にする］ページで、Access Controllerサーバーで実行されている認証サービスのURLを一覧に追加します。一覧に複数のサーバーのURLを追加すると、その順番に基づいてフェールオーバーされます。［Next］をクリックします。
   StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

7. XenDesktopおよびXenAppが提供するリソースをストアで使用できるようにするには、[Secure Ticket Authority（STA）] ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
   STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

8. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

9. ［作成］をクリックします。これにより、［リモートアクセス］ページの一覧にNetScaler Gatewayの展開環境が追加されます。

クラスターをさらに追加する場合は、上記手順を繰り返します。NetScaler Gateway 10.1、Access Gateway 10、Access Gateway 9.3、またはスタンドアロンAccess Gateway 5.0アプライアンスを介したリモートアクセスを構成するには、「NetScaler Gatewayアプライアンスを介したストアへのリモートアクセスを有効にする」の手順に従います。NetScaler Gatewayの展開環境をすべてストアに追加したら、このトピック冒頭の「新しい展開環境の作成」の手順10.以降に従います。

Join an existing server group

May 22, 2017

Before installing StoreFront, ensure that the server you are adding to the group is running the same operating system version with the same locale settings as the other servers in the group. StoreFront server groups containing mixtures of operating system versions and locales are not supported. While a server group can contain a maximum of five servers, from a capacity perspective based on simulations, there is no advantage of server groups containing more than three servers. In addition, ensure that the relative path to StoreFront in IIS on the server you are adding is the same as on the other servers in the group.

> ## Important
>
> When you add a new server to a server group, StoreFront service accounts are added as members of the local administrators group on the new server. These services require local administrator permissions to join and synchronize with the server group. If you use Group Policy to prevent addition of new members to the local administrator group or if you restrict the permissions of the local administrator group on your servers, StoreFront cannot join a server group.

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, on the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. In the results pane of the Citrix StoreFront management console, click Join existing server group.
3. Log on to a server in the StoreFront deployment that you wish to join and open the Citrix StoreFront management console. Select the Server Group node in the left pane of the console and, in the Actions pane, click Add Server. Make a note of the authorization code that is displayed.
4. Return to the new server and, in the Join Server Group dialog box, specify the name of the existing server in the Authorizing server box. Enter the authorization code obtained from that server and click Join.
   Once joined to the group, the configuration of the new server is updated to match the configuration of the existing server. All the other servers in the group are updated with details of the new server.

To manage a multiple server deployment, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Any configuration changes you make must be propagated to the other servers in the group to ensure a consistent configuration across the deployment.

If a StoreFront server was a member of a server group and has been removed, you must run the Clear-DSConfiguration PowerShell cmdlet to reset the StoreFront server to a factory default state. After you run the Clear-DSConfiguration cmdlet on the disconnected server, you can add the server back to an existing server group or to a different newly created server group.

1. Open the StoreFront administration console on the primary StoreFront server that you use to manage your entire server group.
2. Select the server group node on the left pane and choose another server to remove.
3. Remove the selected server from the server group.
4. In the Actions pane, propagate changes from the server you used to disconnect one of your server group members. Any other remaining server group members are now aware that a server has been removed from the group. Until you reset

the disconnected server to a factory default state, it is not aware that it is no longer a member of the group.

5. Close the administration console on the disconnected server.
6. Open a PowerShell session on your disconnected server after it has been removed from the group and import the StoreFront PowerShell modules using: & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"
7. Run the Clear-DSConfiguration command, which resets the server to default settings.
8. Open the StoreFront administration console and the disconnected server is reset and ready to be added to another server group.

Migrate Web Interface features to StoreFront

May 22, 2017

Many of the Web Interface customizations have equivalents in StoreFront by using JavaScript tweaks, Citrix published APIs, or the StoreFront management console.

The table contains an overview of the customizations and basic information about how to achieve them.

- For script customizations, append the examples to the script.js file found in

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

- For style customization, append the example to the style.css file found in

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

- For dynamic content, add the dynamic context to a text file in

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

- If you have a multiserver deployment, you can replicate any changes to other servers from the StoreFront administration console or by using PowerShell.

Note: Web Interface enabled individual users to customize various settings. Currently, StoreFront does not have this ability, and while it is possible to add more extensive customization to support it, that is not the focus of this article.

Web Interface Feature	StoreFront Equivalent
Customization with the Management Console	
• Layout-low graphics • Layout-full graphics • Allow users to choose	Not applicable. StoreFront auto detects and adjusts the UI to device screen.

• Enable search
• Disable search
	• Search is enabled by default.
	• Disable. To hide the search boxes on the desktop/web UI, add the following style to style.css:
	`.search-container {`
	`display: none;`
	`}`

	To hide the search boxes on the phone UI, add:
	`#searchBtnPhone {`
	`display: none;`
	`}`

Enable refresh	Enabled by default (browser refresh).

Enable return to last folder	Not enabled by default.
	Enable Return to last folder - To remember the current folder, and return to it on load, add the following to script.js
	`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);
	}
	};
	});
	};

Enable hints	Citrix Receiver makes very limited use of tool tips, as it is targeting touch and non-touch devices. You can add tool tips by custom script.
• Icon view • Tree view • Details view • List view • Group view • Set Default view • (Low graphics) Icon view • (Low graphics) List view (Low graphics) Default view	Citrix Receiver has a different UI so these choices do not apply. You can use use the StoreFront management console to configure views. For more information see, Specify different views for applications and desktops.

• Single tab UI
• Tabbed UI
  • App tab
  • Desktop tab
	The Citrix Receiver UI is tabbed by default, with apps and content in one tab and desktops in the other. There is also an optional **Favorite** tab.

• Content tab • (Tab order)	

• Header logo
• Text color
• Header background color
• Header background image
	Equivalents for colors and logos using the StoreFront administration console. Click Customize Website Appearance in the StoreFront administration console's Actions pane and make your customizations on the screen that displays.
	
	You can set the header to a background image using a style customization. For example
	
	.theme-header-bgcolor {
	
	background-image: url('spirals.png');
	
	}

• Pre-logon welcome message (Pre-locale)
  • Title
  • Text
  • Hyperlink
  • Button label
	By default, there is no separate pre-logon screen.
	
	This example script adds a click-through message box:
	
	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();
	}
	};

• Logon screen title
• Logon screen message
• Logon screen system message
	There are four areas for customization on the logon screen(s). Top and bottom of screen (header and footer) and top and bottom of the logon box itself.
	.customAuthHeader,
	.customAuthFooter
	.customAuthTop,
	.customAuthBottom {
	text-align: center;
	color: white;
	font-size: 16px;
	}
	Example script (static content)
	$('.customAuthHeader').html("Welcome to ACME");
	Example script (dynamic content)
	function setDynamicContent(txtFile, element) {
	CTXS.ExtensionAPI.proxyRequest({
	url: "customweb/"+txtFile,
	success: function(txt) {$(element).html(txt);}});
	}
	setDynamicContent("Message.txt", ".customAuthTop");

	Note: Do not explicitly include dynamic content in the script, or put it in the **custom** directory, as changes made here force all clients to reload the UI. Put dynamic content in the **customweb** directory.
• Application screen welcome message • Application screen system message	See the examples for **CustomAuth** welcome screen above. See examples for dynamic content above. Use '**#customTop**' rather than '**.customAuthTop**' to place content on the home screen.
Footer text (all screens)	Example script: **#customBottom {** **text-align: center;** **color: white;** **font-size: 16px;** **}** Example static content using a script: **$('#customBottom').html("Welcome to ACME");**
Features with no direct equivalent	
• Logon screen without headers • Logon screen with headers (including messages)	There is no direct equivalent in StoreFront. However, you can create custom headers. See "Logon Screen Title" above.
User settings	By default, there are no user settings. You can add menus and buttons from JavaScript.
Workspace control	Equivalent functionality for administrator settings. The extension APIs allow significant additional flexibility. See http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html.
Deep Customizations (code)	

ICA File generation hooks and other call-routing customizations.	Equivalent or better APIs. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
Authentication customizations	Equivalent or better APIs. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
JSP/ASP source access	There are no equivalent APIs on StoreFront, as the UI is not rendered in the same way. There are many JavaScript APIs to enable customization of the UI.

サーバーグループの構成

May 22, 2017

以下のタスクでは、複数サーバーのStoreFront展開環境の設定を変更します。複数サーバー展開環境を管理する場合、同時に複数のサーバー上でサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。また、展開環境内で一貫した構成を保つため、構成の変更内容をグループ内のほかのサーバーに反映させる必要があります。

StoreFrontサーバーグループに含まれるサーバーは、StoreFrontのインストール場所の設定とIIS Webサイトの設定（物理パスやサイトIDなど）の両方が同じになるように構成する必要があります。

［サーバーの追加］タスクを使用して、新しくインストールしたStoreFrontサーバーを既存の展開環境に追加するための承認コードを取得します。新しいサーバーを既存のStoreFront展開環境に追加する方法について詳しくは、「既存のサーバーグループへの参加」を参照してください。グループ内のいくつのサーバーにアクセスする必要があるかについては、「StoreFrontの展開計画」の「*スケーラビリティ*」の説明を参照してください。

複数サーバーのStoreFront展開環境からサーバーを削除するには、［サーバーの削除］タスクを使用します。このタスクでは、StoreFront管理コンソールを実行しているサーバー以外の任意のサーバーをグループから削除できます。ただし、複数サーバーの展開環境からサーバーを削除する前に、そのサーバーを負荷分散環境から削除しておく必要があります。

現在のサーバー上で行った変更内容を、複数サーバーのStoreFront展開環境内のほかのすべてのサーバーに反映させるには、［変更の伝達］タスクを使用します。これにより、グループ内のほかのサーバー上で行ったすべての変更が破棄されます。このタスクの実行中は、グループ内のすべてのサーバーが更新されるまで、追加の変更を加えることはできません。

重要：サーバーの構成を変更してからグループ内のほかのサーバーにその変更を反映させないと、後で展開環境内の別のサーバーでの変更が反映された場合に元の変更内容が失われる可能性があります。

StoreFront展開環境でホストされるストアやほかのStoreFrontサービスのルートURLを変更するには、[ベースURLの変更］タスクを使用します。複数サーバーの展開環境の場合は、負荷分散URLを指定します。Microsoftインターネットインフォメーションサービス（IIS）でHTTPSが正しく構成されている場合は、［ベースURLの変更］タスクでHTTPをHTTPSに変更することもできます。

IISでHTTPSを構成するには、StoreFrontサーバー上でインターネットインフォメーションサービス（IIS）マネージャーコンソールを使用して、Microsoft Active Directoryドメイン証明機関により署名されたサーバー証明書を作成します。次に、HTTPSバインドをデフォルトのWebサイトに追加します。IISでのサーバー証明書の作成について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831637.aspx#CreateCertificateを参照してください。IISサイトへのHTTPSバインドの追加について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831632.aspx#SSLBindingを参照してください。

リソースを提供するサーバーの一部が使用できなくなったときのパフォーマンスを向上させるために、応答しないサーバーがStoreFrontにより一時的にバイパスされます。バイパスされたサーバーはStoreFrontにより無視され、リソースのアクセスに使用されません。このバイパスの期間は、次のパラメーターで指定します。

- **[すべての失敗のバイパス時間]** では、特定のDelivery Controllerのすべてのサーバーがバイパスされている場合に、**[バイパス時間]** の代わりに適用される短い期間を分単位で指定します。デフォルトは10分です。
- **[バイパス時間]** では、特定のサーバーへの接続に失敗した後で、StoreFrontがそのサーバーをバイパスする期間を分単位で指定します。デフォルトのバイパス時間は60分間です。

[すべての失敗のバイパス時間] 指定時の考慮事項

[すべての失敗のバイパス時間] を長く設定すると、特定のDelivery Controllerを使用できないことによる影響を小さくすることができますが、一時的なネットワーク障害やサーバー障害の後で、ユーザーがこのDelivery Controllerのリソースをその期間使用できなくなるという悪影響もあります。多くのDelivery Controllerを単一のストア用に構成している場合、特に、業務に重要ではないDelivery Controllerの場合は、 **[すべての失敗のバイパス時間]** の値を大きめにすることを検討してください。

[すべての失敗のバイパス時間] を短くするとそのDelivery Controllerで提供されるリソースの可用性は高まりますが、単一のストアを構成する多くのDelivery Controllerのうちの複数台が使用できない場合に、クライアント側でタイムアウトが発生しやすくなります。少数のファームを構成していて、業務に重要なDelivery Controllerの場合は、デフォルト値の0分を使用することをお勧めします。

ストアのバイパスパラメーターを変更するには

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[Delivery Controllerの管理]** をクリックします。
3. Controllerを選択し、 **[編集]** をクリックして、 **[Delivery Controllerの編集]** 画面の **[設定]** をクリックします。
4. **[すべての失敗のバイパス時間]** の行で2列目をクリックし、サーバーがすべて応答できなくなってからDelivery Controllerがオフラインとみなされるまでの時間を分単位で入力します。
5. **[バイパス時間]** の行で2列目をクリックし、単一のサーバーが応答しなくってからオフラインとみなされるまでの時間を分単位で入力します。

認証と委任の構成

May 22, 2017

自分の要件によって、複数の認証と委任法方式があります。

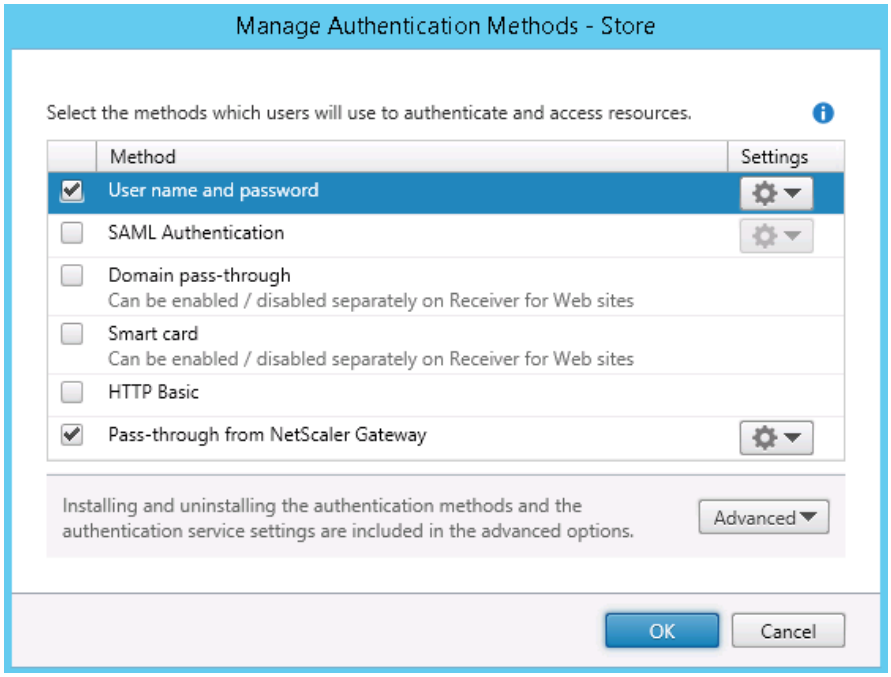
認証サービスの構成	認証サービスにより、ユーザーがMicrosoft Active Directoryで認証され、ユーザーが再ログオンすることなくデスクトップやアプリケーションにアクセスできるようになります。
XMLサービスベースの認証	StoreFrontがXenAppまたはXenDesktopと同じドメイン内にない場合、またActive Directoryの信頼を適切に配置できない場合には、XenAppおよびXenDesktop XML Serviceを使ってユーザー名とパスワード資格情報を認証するようにStoreFrontを構成できます。
XenApp 6.5のKerberos制約付き委任。	StoreFrontでDelivery Controllerの認証に単一ドメインKerberos制約付き委任を使用するかどうかを指定するには、［Kerberos委任の構成］タスクを使用します。
スマートカード認証	一般的なStoreFront展開のすべてのコンポーネントに対するスマートカード認証をセットアップします。
パスワードの有効期限切れ通知期間	Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。

認証サービスの構成

May 22, 2017

ユーザーの認証方法を有効にしたり無効にしたりするには、Citrix StoreFront管理コンソールの結果ペインで認証方法を選択して、［操作］ペインの［認証方法の管理］をクリックします。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix**StoreFront**］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、**[操作]** ペインの **[認証方法の管理]** をクリックします。
3. ユーザーに許可するアクセス方法を指定します。



- 指定ユーザー認証を有効にするには **[ユーザー名とパスワード]** チェックボックスをオンにします。この場合、ユーザーは資格情報を入力してストアにアクセスします。
- SAML IDプロバイダーとの統合を有効にするには、**[SAML認証]** チェックボックスをオンにします。ユーザーはAccess Gatewayにログオンすることによって認証を受け、ストアにアクセスするときは自動的にログオンします。 ［設定］ボックスの一覧で次を選択します。
  - **IDプロバイダー**：IDプロバイダーの信頼性を構成する場合。
  - **サービスプロバイダー**：サービスプロバイダーの信頼性を構成する場合。この情報は、IDプロバイダーから要求されます。
- ユーザーデバイスからActive Directoryドメイン資格情報がパススルーされるようにするには、[ドメインパススルー] チェックボックスをオンにします。

この場合、ユーザーはドメインに参加しているWindowsコンピューターにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。このオプションを使用する場合は、Citrix Receiver for Windowsをユーザーデバイスにインストールするときにパススルー認証を有効にする必要があります。

- スマートカード認証を有効にするには、［スマートカード］チェックボックスをオンにします。ユーザーはスマートカードとPINを使ってストアにアクセスします。
- HTTP基本認証を有効にするには、［HTTP基本］チェックボックスをオンにします。ユーザー認証は、StoreFrontサーバーのIIS Webサーバーで実行されます。
- NetScaler Gatewayからのパススルー認証を有効にするには、［NetScaler Gatewayからのパススルー］チェックボックスをオンにします。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。

NetScaler Gatewayを経由してストアにアクセスするスマートカードユーザーのパススルー認証を有効にするには、［認証の委任構成］タスクを使用します。

信頼されるユーザードメインの構成

ドメインの資格情報を明示的に入力して（直接またはNetScaler Gatewayを介したパススルー認証で）ログオンするユーザーのストアへのアクセスを制限するには、［信頼されるドメイン］タスクを使用します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインで認証方法を選択します。［操作］ペインで **［認証方法の管理］** をクリックします。
3. **［ユーザー名とパスワード（明示的）］＞［設定］** ドロップダウンメニューから、**［信頼されるドメイン**の構成］を選択します。
4. **［信頼済みドメインのみ］** をクリックして［追加］をクリックし、信頼されるドメインの名前を入力します。この認証サービスを使用するすべてのストアでは、ここで追加したドメインのアカウントでログオンできるようになります。ドメインを変更するには、［信頼されるドメイン］の一覧でエントリを選択して［編集］をクリックします。特定ドメインのユーザーアカウントでのアクセスを禁止するには、一覧でそのドメインを選択して［削除］をクリックします。
   管理者がドメイン名を指定する方法により、ユーザーが資格情報の入力時に使用すべき形式が決まります。ユーザーにドメインユーザー名形式で資格情報を入力させるには、一覧にNetBIOS名を追加します。ユーザーにユーザープリンシパル名形式で資格情報を入力させるには、一覧に完全修飾ドメイン名を追加します。ユーザーがドメインユーザー名形式でもユーザープリンシパル名形式でも資格情報を入力できるようにするには、一覧にNetBIOS名と完全修飾ドメイン名の両方を追加する必要があります。
5. 信頼されるドメインを複数構成する場合は、ユーザーがログオンするときにデフォルトで選択されるドメインを[デフォルトドメイン］ボックスの一覧から選択します。
6. ログオンページに信頼されるドメインを一覧表示するには、［ログオンページにドメイン一覧を表示する］チェックボックスをオンにします。

ユーザーがパスワードを変更できるようにする

ドメインの資格情報を使ってデスクトップのReceiverとReceiver for Webサイトにログオンするユーザーがパスワードを変更できるようにするには、**［パスワードオプションの管理］** タスクを使用します。認証サービスを作成したときのデフォルトの構成では、パスワードが失効しても、Citrix ReceiverとCitrix Receiver for Webサイトのユーザーはパスワードを変更できません。この機能を有効にする場合は、サーバーが属しているドメインのポリシーでユーザーによるパスワード変更が禁止されていないことを確認してください。ユーザーによるパスワードの変更を有効にすると、この認証サービスを使用するストアにアクセスできるすべてのユーザーに、慎重に扱うべきセキュリティ機能が公開されることになります。組織のセキュリティポリシーにより、ユーザーパスワード変更機能が内部使用のみに制限される環境では、社内ネットワークの外側からそれらのストアにアクセスできないことを確認してください。

1. Citrix Receiver for Webは、選択的なパスワードの変更に加えて、有効期限が切れた時のパスワードの変更をサポートします。すべてのデスクトップCitrix Receiverは、有効期限が切れた時にのみNetScaler Gatewayを介したパスワードの変更を

ポートします。Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。

2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの［認証方法の管理］をクリックします。
3. **［ユーザー名とパスワード］** > **［設定］** ドロップダウンメニューから、**[パスワードオプションの管理]** を選択し、ドメインの資格情報を使ってCitrix Receiver for Webサイトにログオンするユーザーに、パスワードの変更を許可する条件を指定します。
   - ユーザーがいつでもパスワードを変更できるようにするには、［常時］を選択します。パスワードの期限切れが近いローカルユーザーには、ログオン時に警告が表示されます。パスワードの有効期限切れの警告は、内部ネットワークから接続しているユーザーにのみ表示されます。デフォルトでは、ユーザーに対する通知期間は、適用されるWindowsポリシーの設定によって決まります。この通知期間の設定について詳しくは、「パスワードの有効期限切れ通知期間の構成」を参照してください。Citrix Receiver for Webでのみサポートされます。
   - 有効期限切れのパスワードだけをユーザーが変更できるようにするには、［失効したとき］を選択します。パスワードが失効してログオンできなくなったユーザーには、［パスワードの変更］ダイアログボックスが開きます。デスクトップのCitrix ReceiverとCitrix Receiver for Webでサポートされます。
   - ユーザーによるパスワードの変更を禁止するには、**[ユーザーにパスワードの変更を許可する]** の選択を解除します。このオプションを選択しない場合は、パスワードが失効してデスクトップやアプリケーションにアクセスできないユーザーをどのようにサポートするかを検討しておく必要があります。

   Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように構成する場合は、StoreFrontサーバー上にすべてのユーザーのプロファイルを保存するための空き領域があることを確認してください。StoreFrontではユーザーのパスワードの失効が近いかどうかを確認するため、サーバー上に各ユーザーのローカルプロファイルが作成されます。ユーザーのパスワードを変更するには、StoreFrontはドメインコントローラーと通信する必要があります。

Citrix Receiver	StoreFrontで有効になっている場合、ユーザーが有効期限切れのパスワードできる	パスワードの有効期限が切れたら、ユーザーに通知される	StoreFrontで有効になっている場合は、パスワードの有効期限が切れる前に、ユーザーがそれを変更できる
Windows：	はい		
Mac：	はい		
Android			
iOS			
Linux：	はい		
Web	はい	はい	はい

セルフサービスパスワードリセットにより、エンドユーザーは自身のユーザーアカウントをより詳細に制御できるようになります。セルフサービスパスワードリセットが構成されると、エンドユーザーは、システムへのログオンで問題がある場合にいくつかのセキュリティの質問に答えることによって、アカウントのロックを解除するか、パスワードをリセットして新しいパスワードを設定できます。

セルフサービスパスワードリセットのセットアップ時に、管理コンソールを使用してパスワードのリセットとアカウントのロック解除を許可するユーザーを指定します。StoreFrontでこれらの機能を有効にしても、セルフサービスパスワードリセットの設定で許可されていないユーザーは、これらの操作を行うことができません。

セルフサービスパスワードリセットは、ユーザーがHTTPS接続を使ってStoreFrontにアクセスする場合にのみ使用できます。ユーザーは、HTTP接続とセルフサービスパスワードリセットを使用しても、StoreFrontにアクセスすることはできません。セルフサービスパスワードリセットは、ユーザー名とパスワードでStoreFrontに直接認証する場合にのみ利用できます。

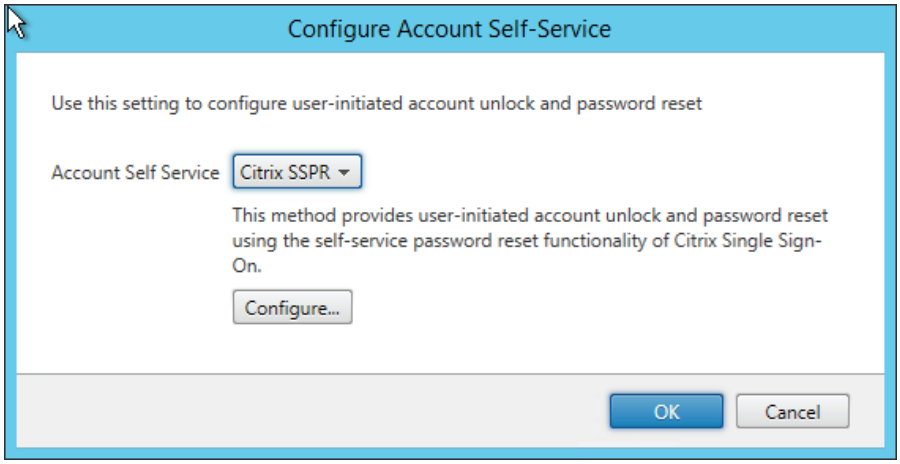
セルフサービスパスワードリセットでは、username@domain.comなどのUPNログオンはサポートされません。

ストアのセルフサービスパスワードリセットを設定する前に、次のことを確認する必要があります。

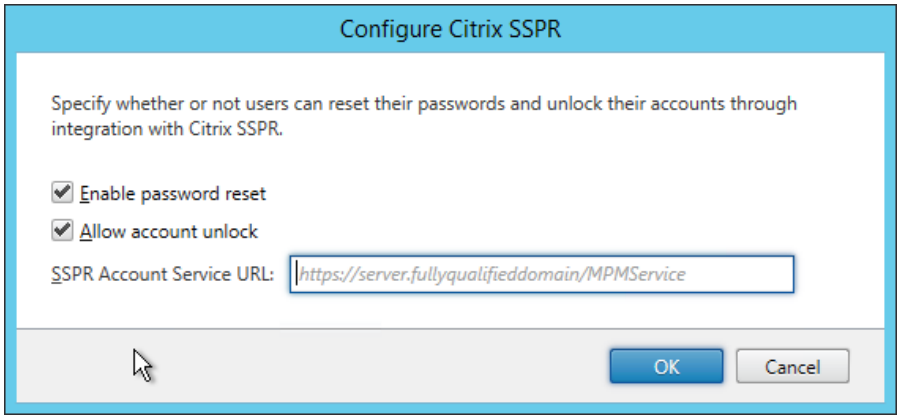
- ストアが、ユーザー名とパスワードによる認証を使用するように構成されている。
- ストアが、1つのセルフサービスパスワードリセットのみを使用するように構成されている。StoreFrontが、複数の同じドメインまたは信頼されているドメイン内にある複数のサーバーファームを使用するように構成されている場合は、これらすべてのドメインの資格情報を受け入れるようにセルフサービスパスワードリセットを構成する必要があります。
- ストアが、ユーザーがパスワードを常時変更できるように構成されている（パスワードのリセット機能を有効にする場合）。
- StoreFrontストアをReceiver for Webサイトに割り当てる必要があり、そのサイトが統合エクスペリエンスを使用するように構成する必要がある。

セルフサービスパスワードリセットを使用できるようにするには、インストールして構成する必要があります。XenApp 7.11およびXenDesktop 7.11のメディアで可能です。詳しくは、「セルフサービスパスワードリセット」を参照してください。

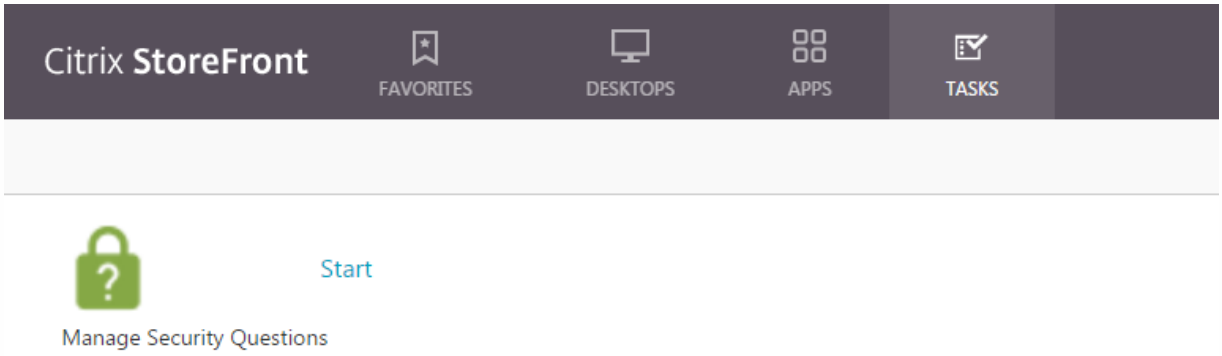
1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[認証方法の管理]** > **[ユーザー名とパスワード]** をクリックし、ドロップダウンメニューから **[パスワードオプションの管理]** を選択します。
2. パスワードの変更を許可するユーザーを選択し、 **[OK]** をクリックします。
3. **[ユーザー名とパスワード]** ボックスの一覧で **[アカウントセルフサービスの設定]** を選択し、ドロップダウンメニューで **[Citrix SSPR]** を選択して **[OK] をクリックします。**
4. ユーザーに対して、セルフサービスパスワードリセットを使用したパスワードのリセットおよびアカウントのロック解除を許可するかどうかを指定して、パスワードリセットサービスのアカウントURLを追加し **[OK]** 、そして **[OK] をクリックします。**



このオプションは、StoreFrontベースのURLがHTTPS（HTTPではない）の場合にのみ利用可能であり、**[パスワードリセットを有効にする]** オプションは、 **[パスワードオプションの管理]** を使用してユーザーがいつでもパスワードを変更できるようにした後でのみ利用可能です。



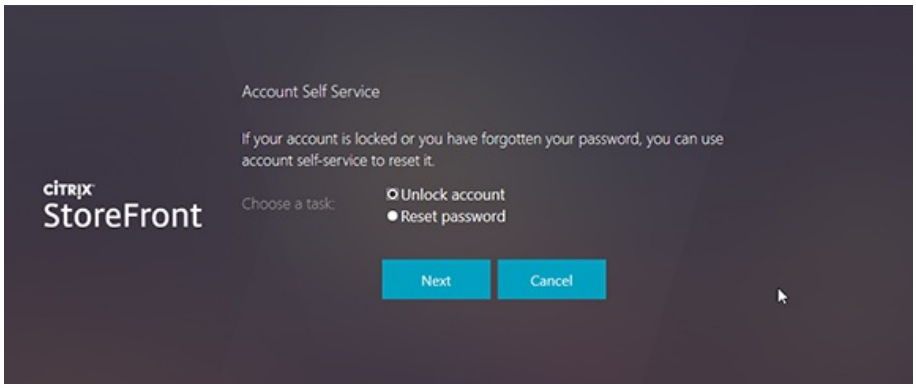
CitrixReceiverまたはCitrix Receiver for Webへの次回ユーザーログオン時に、セキュリティ用の質問に対する回答を登録できるようになります。 **[開始]** をクリックすると、ユーザーが回答を登録する必要のある質問が表示されます。



StoreFrontでの設定後、Citrix Receiver for Webのログオン画面に **[アカウントセルフサービス]** リンクが表示されるようになります（ほかのCitrix Receiverではボタンとして表示されます）。

このリンクをクリックすると、 **[アカウントのアンロック]** と **[パスワードのリセット]** （両方とも利用可能な場合）の間で、最初に選択する一連のフォームが表示されます。

ラジオボタンを選択して **[次へ]** をクリックすると、次の画面ではドメインとユーザー名（*ドメイン\ユーザー*）の入力を求められます（この情報がログオンフォームで入力されていない場合）。アカウントセルフサービスでは、username@domain.comなどのUPNログオンはサポートされないことに注意してください。



ユーザーは、セキュリティの質問に回答するように求められます。すべての回答が、ユーザーが入力した回答と一致すると、要求した操作（ロック解除またはリセット）が実行され、操作に成功したことを示すメッセージが表示されます。

共有認証サービス設定

共有認証サービス設定タスクを使ってストアを指定し、ストア間でシングルサインオンを有効にする認証サービスを共有します。

1. Windowsの［**スタート**］画面または［**アプリ**］画面で、［**Citrix StoreFront**］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［**ストア**］ノードを選択して、結果ペインでストアを選択します。［**操作**］ペインで［**認証方法の管理**］をクリックします。
3. ［**詳細**］ドロップダウンメニューから、［**共有認証サービス設定**］を選択します。
4. ［**共有認証サービスを使用する**］チェックボックスをオンにして、［**ストア**］名ドロップダウンメニューからストアを選択します。

注：共有認証サービスと専用認証サービス間には機能的な差異はありません。2つ以上のストアによって共有される認証サービスは、共有認証サービスとして扱われ、構成の変更はいずれも共有認証サービスを使用するすべてのストアに対して適用されます。

資格情報の検証をNetScaler Gatewayに委任する

NetScaler Gatewayを経由してストアにアクセスするスマートカードユーザーのパススルー認証を有効にするには、［認証の委任構成］タスクを使用します。このタスクは、［NetScaler Gatewayからのパススルー］が有効で、その認証方法が結果ペインで選択されている場合のみ使用できます。

資格情報の検証をNetScaler Gatewayに委任した場合、ユーザーはスマートカードを使ってNetScaler Gatewayにログオンし、ストアにアクセスするときは自動的に認証されます。スマートカードユーザーのパススルー認証は、管理者がNetScaler Gatewayからのパススルー認証を有効にするとデフォルトで無効になるため、ユーザーがパスワードを使ってNetScaler Gatewayにログオンした場合にのみパススルー認証が発生します。

XMLサービスベースの認証

May 22, 2017

StoreFrontがXenAppまたはXenDesktopと同じドメイン内にない場合、またActive Directoryの信頼を適切に配置できない場合には、XenAppおよびXenDesktop XML Serviceを使ってユーザー名とパスワード資格情報を認証するようにStoreFrontを構成できます。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの **[認証方法の管理]** をクリックします。
3. **[認証方法の管理]** ページで、 **[ユーザー名とパスワード]** > **[設定]** ドロップダウンメニューから、 **[パスワード確認の構成]** を選択します。
4. **[パスワード検証方法]** ドロップダウンメニューから **[Delivery Controller]** を選択し、 **[構成]** をクリックします。
5. **[Delivery Controllerの構成]** 画面に従って、1つまたは複数のDelivery Controllerを追加して、ユーザー資格情報を確認し、 **[OK]** をクリックします。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの **[認証方法の管理]** をクリックします。
3. **[認証方法の管理]** ページで、 **[ユーザー名とパスワード]** > **[設定]** ドロップダウンメニューから、 **[パスワード確認の構成]** を選択します。
4. **[パスワード検証方法]** ドロップダウンメニューから **[Active Directory]** を選択し、 **[OK]** をクリックします。

Configure Kerberos constrained delegation for XenApp 6.5

May 22, 2017

Use the **Configure Store Settings > Kerberos delegation** task to specify whether StoreFront uses single-domain Kerberos constrained delegation to authenticate to delivery controllers.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click **Configure Store Settings,** and then click Kerberos Delegation.
3. Select Enable or Disable Kerberos delegation to authenticate to delivery controllers, respectively, enable or disable Kerberos constrained delegation.

Follow this procedure when StoreFront is not installed on the same machine as XenApp.

1. On the domain controller, open the MMC Active Directory Users and Computers snap-in.
2. On the View menu, click Advanced Features.
3. In the left pane, click the Computers node under the domain name and select the StoreFront server.
4. In the Action pane, click Properties.
5. On the Delegation tab, click Trust this computer for delegation to specified services only and Use any authentication protocol, and then click Add.
6. In the Add Services dialog box, click Users or Computers.
7. In the Select Users or Computers dialog box, type the name of the server running the Citrix XML Service (XenApp) in the Enter the object names to select box, click OK.
8. Select the HTTP service type from the list, click OK.
9. Apply the changes and close the dialog box.

Configure Active Directory Trusted Delegation for each XenApp server.

1. On the domain controller, open the **MMC Active Directory Users and Computers** snap-in.
2. In the left pane, click the **Computers** node under the domain name and select the server running the Citrix XML Service (XenApp) that StoreFront is configured to contact.
3. In the **Action** pane, click **Properties**.
4. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use any authentication protocol**, and then click **Add**.
5. In the **Add Services** dialog box, click **Users or Computers**.
6. In the **Select Users or Computers** dialog box, type the name of the server running the Citrix XML Service (XenApp) in the **Enter the object names to select** box, click **OK**.
7. Select the HOST service type from the list, click **OK**, and then click **Add**.

8. In the **Select Users or Computers** dialog box, type the name of the Domain Controller in the **Enter the object names to select box** and click **OK**.
9. Select the **cifs** and **ldap** service types from the list and click **OK**. Note: If two choices appear for the ldapservice, select the one that matches the FQDN of the domain controller.
10. Apply the changes and close the dialog box.

Important considerations

When you decide whether to use Kerberos constrained delegation, consider the following information.

- Key Notes:
  - You do not need ssonsvr.exe unless doing pass-through authentication (or smart card pin pass-through authentication) without Kerberos constrained delegation.
- Storefront and Citrix Receiver for Web domain pass-through:
  - You do not need ssonsvr.exe on the client.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Add the Storefront Fully Qualified Domain Name (FQDN) to Internet Explorer trusted sites list. Check the Use local username box in the Internet Explorer security settings for the trusted zone.
  - The client must be in a domain.
  - Enable the Domain pass-through authentication method on the StoreFront server and enable for Citrix Receiver for Web.
- Storefront, Citrix Receiver for Web, and smart card authentication with PIN prompt:
  - You do not need ssonsvr.exe on the client.
  - Smart card authentication was configured.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Enable the Smart card authentication method on the StoreFront server and enable for Citrix Receiver for Web.
  - To ensure smart card authentication is chosen, do not check the Use local username box in the Internet Explorer security settings for the StoreFront site zone.
  - The client must be in a domain.
- NetScaler Gateway, StoreFront, Citrix Receiver for Web, and smart card authentication with PIN prompt:
  - You do not need ssonsvr.exe on the client.
  - Smart card authentication was configured.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Enable the Pass-through from NetScaler Gateway authentication method on the StoreFront server and enable for Citrix Receiver for Web.
  - To ensure smart card authentication is chosen, do not check the Use local username box in the Internet Explorer security settings for the StoreFront site zone.
  - The client must be in a domain.
  - Configure NetScaler Gateway for smart card authentication and configure an additional vServer for launch using StoreFront HDX routing to route the ICA traffic through the unauthenticated NetScaler Gateway vServer.
- Citrix Receiver for Windows (AuthManager), smart card authentication with PIN prompt, and StoreFront:
  - You do not need ssonsvr.exe on the client.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - The client must be in a domain.
  - Enable the Smart card authentication method on the StoreFront server.
- Citrix Receiver for Windows (AuthManager), Kerberos, and StoreFront:
  - You do not need ssonsvr.exe on the client.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Check the Use local username box in the Internet Explorer security settings for the trusted zone.
  - The client must be in a domain.
  - Enable the Domain pass-through authentication method on the StoreFront server.
  - Ensure this registry key is set:

    Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindows
Name: SSONCheckEnabled
Type: REG_SZ
Value: true or false

For 64-bit machines:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\integratedwindows

Name: SSONCheckEnabled
Type: REG_SZ
Value: true or false

スマートカード認証の構成

May 22, 2017

このトピックでは、一般的なStoreFront展開環境のすべてのコンポーネントでスマートカード認証を設定するための概要について説明します。詳細と構成手順については、各製品のドキュメントを参照してください。

Citrix環境のスマートカード構成

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

- StoreFrontサーバーを展開するMicrosoft Active Directoryドメインか、そのドメインと直接の双方向の信頼関係が設定されているドメインのいずれかにすべてのユーザーアカウントが属していることを確認します。
- スマートカードパススルー認証を有効にする場合は、スマートカードリーダーの種類、ミドルウェアの種類と構成、およびミドルウェアのPINのキャッシュポリシーでパススルー認証が許可されることを確認します。
- ユーザーのデスクトップやアプリケーションを提供する、Virtual Delivery Agentが動作する仮想マシンや物理マシンに、スマートカードのベンダーが提供するミドルウェアをインストールします。XenDesktop環境でスマートカードを使用する方法については、「スマートカードによる認証セキュリティ」を参照してください。
- 事前に公開キーインフラストラクチャが正しく構成されていることを確認します。アカウントマッピングのための証明書がActive Directory環境に対して正しく構成されており、ユーザー証明書の検証を正しく実行できることを確認します。

- NetScaler Gatewayアプライアンスに、証明機関からの署名入りサーバー証明書をインストールします。詳しくは、「Installing and Managing Certificates」を参照してください。
- アプライアンスに、スマートカードユーザーの証明書を発行した証明機関のルート証明書をインストールします。詳しくは、「To install a root certificate on NetScaler Gateway」を参照してください。
- クライアント証明書認証用の仮想サーバーを作成して構成します。証明書認証ポリシーを作成し、証明書のユーザー名抽出オプションとして「SubjectAltName:PrincipalName」を指定します。さらに、このポリシーを仮想サーバーにバインドして、クライアント証明書を要求するように構成します。詳しくは、「Configuring and Binding a Client Certificate Authentication Policy」を参照してください。
- 証明機関のルート証明書を仮想サーバーにバインドします。詳しくは、「To add a root certificate to a virtual server」を参照してください。
- 資格情報を再入力せずにリソースに接続されるようにするには、仮想サーバーをもう1つ作成し、SSL（Secure Sockets Layer）パラメーターでクライアント認証を無効にします。詳しくは、「スマートカード認証の構成」を参照してください。
  管理者は、作成した仮想サーバー経由でユーザー接続がルーティングされるようにStoreFrontを構成する必要もあります。ユーザーは最初の仮想サーバーにログオンします。作成した（2つ目の）仮想サーバーはリソースへの接続に使用されます。接続時にNetScaler Gatewayにログオンする必要はありませんが、デスクトップやアプリケーションへのログオン時にPINを入力する必要があります。スマートカードでの認証の失敗時に指定ユーザー認証を使用できるように設定する場合を除き、2つ目の仮想サーバーをリソースへのユーザー接続用に構成することは省略可能です。

- NetScaler Gateway経由でStoreFrontに接続するためのセッションポリシーおよびセッションプロファイルを作成して、それらを適切な仮想サーバーにバインドします。詳しくは、「Access to StoreFront Through NetScaler Gateway」を参照してください。
- StoreFrontへの接続用の仮想サーバーを構成するときに、すべての通信がクライアント証明書で認証されるように指定した場合は、StoreFrontのコールバックURLを提供する仮想サーバーをさらに作成する必要があります。この仮想サーバーは、

StoreFrontでNetScaler Gatewayアプライアンスからの要求を検証するためだけに使用されるため、公開ネットワークからアクセス可能である必要はありません。クライアント証明書による認証が必要な場合は、隔離された仮想サーバーが必要です。これは、認証用の証明書をStoreFrontで提示できないためです。詳しくは、「仮想サーバーの作成」を参照してください。

- スマートカード認証を有効にするには、StoreFrontとユーザーデバイス間の通信でHTTPSが使用されるように構成する必要があります。Microsoftインターネットインフォメーションサービス（IIS）でHTTPSを構成します。これを行うには、IISでSSL証明書を入手して、HTTPSバインドをデフォルトのWebサイトに追加します。IISでのサーバー証明書の作成について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831637.aspx#CreateCertificateを参照してください。IISサイトへのHTTPSバインドの追加について詳しくは、http://technet.microsoft.com/ja-jp/library/hh831632.aspx#SSLBindingを参照してください。
- すべてのStoreFront URLへのHTTPS接続でクライアント証明書が要求されるようにするには、StoreFrontサーバー上でIISを構成します。
  StoreFrontインストール時のIISのデフォルト構成では、StoreFront認証サービスの証明書認証URLへのHTTPS接続でのみクライアント証明書が要求されます。この構成は、ユーザーがスマートカードでログオンできない場合に指定ユーザー認証でログオンできるようにしたり、再認証なしにスマートカードを取り出せるようにするために必要です。

  すべてのStoreFront URLへのHTTPS接続でクライアント証明書が要求されるようにIISを構成すると、スマートカードユーザーがNetScaler Gateway経由で接続できなくなり、指定ユーザー認証にもフォールバックされません。また、スマートカードをデバイスから取り出す場合は再度ログオンする必要があります。このIISサイト構成を有効にするには、認証サービスとストアを同じサーバー上に配置して、すべてのストアに対して有効なクライアント証明書を使用する必要があります。また、すべてのStoreFront URLへのHTTPS接続でクライアント証明書が要求されるようにIISを構成すると、Citrix Receiver for Webクライアントでの認証に問題が生じます。このため、Citrix Receiver for Webクライアントを使用しない場合のみ、この構成を使用してください。

  StoreFrontをWindows Server 2012上にインストールして、IISでSSLとクライアント証明書による認証を有効にする場合、サーバー上の「信頼されたルート証明機関」の証明書ストアにインストールされた非自己署名証明書が拒否されることに注意してください。詳しくは、http://support.microsoft.com/kb/2802568を参照してください。

- StoreFrontをインストールして構成します。必要に応じて、認証サービスを作成し、ストアを追加します。NetScaler Gatewayを介したリモートアクセスを有効にする場合は、仮想プライベートネットワーク（VPN）統合を有効にしないでください。詳しくは、「StoreFrontのインストールとセットアップ」を参照してください。
- 内部ネットワーク上のローカルユーザーに対して、StoreFrontへのスマートカード認証を有効にします。スマートカードユーザーがNetScaler Gateway経由でストアにアクセスする場合は、認証方法としてNetScaler Gatewayからのパススルーを有効にして、資格情報の検証をNetScaler Gatewayに委任します。ドメインに参加しているユーザーデバイスにCitrix Receiver for Windowsをインストールするときにパススルー認証を有効にする場合は、ドメインパススルー認証を有効にしておきます。詳しくは、「認証サービスの構成」を参照してください。
  Citrix Receiver for Webクライアントでスマートカードによる認証を許可するには、各Citrix Receiver for Webサイトでこの認証方法を有効にする必要があります。方法については、「Citrix Receiver for Webサイトの構成」を参照してください。

  スマートカード認証で指定ユーザー認証へのフォールバックを有効にする場合は、ユーザー名とパスワードを使用する認証方法を無効にしないでください。

- ドメインに参加しているユーザーデバイスにCitrix Receiver for Windowsをインストールするときにパススルー認証を有効にする場合は、デスクトップやアプリケーションにアクセスするときにスマートカードの資格情報がパススルーされるようにストアのdefault.icaファイルを編集します。詳しくは、「Citrix Receiver for Windowsのスマートカードパススルー認証を有効にする」を参照してください。
- デスクトップやアプリケーションへのユーザー接続のみに使用されるNetScaler Gateway仮想サーバーを追加した場合は、

その仮想サーバーを経由する「最適なNetScaler Gatewayルーティング」を構成します。詳しくは、「ストアの最適なHDX
ルーティングの構成」を参照してください。

- ドメインに不参加のWindowsデスクトップアプライアンスのユーザーがスマートカードを使用してデスクトップにログオンできるようにするには、デスクトップアプライアンスサイトへのスマートカード認証を有効にします。詳しくは、「デスクトップアプライアンスサイトの構成」を参照してください。

  デスクトップアプライアンスサイトでスマートカード認証および指定ユーザー認証の両方を有効にして、スマートカードでログオンできない場合は資格情報を入力してログオン（指定ユーザー認証）できるようにします。

- ドメインに参加しているデスクトップアプライアンスのユーザー、およびCitrix Desktop Lockを実行している再目的化されたPCのユーザーがスマートカードを使用して認証できるようにするには、XenApp Servicesサイトへのスマートカードパススルー認証を有効にします。詳しくは、「XenApp Services URLの認証の構成」を参照してください。

- すべてのユーザーデバイスに、スマートカードのベンダーが提供するミドルウェアをインストールします。
- ユーザーが、ドメインに不参加のWindowsデスクトップアプライアンスを使用する場合は、管理者権限を持つアカウントでReceiver for Windows Enterpriseをインストールします。デバイスの電源を入れたときにInternet Explorerが全画面モードで起動して、デスクトップアプライアンスサイトが表示されるように構成します。デスクトップアプライアンスサイトのURLでは大文字と小文字が区別されることに注意してください。デスクトップアプライアンスサイトをInternet Explorerのローカルイントラネットまたは信頼済みサイトのゾーンに追加します。スマートカードを使用してデスクトップアプライアンスサイトにログオンして、ストアからリソースにアクセスできることを確認した後で、Citrix Desktop Lockをインストールします。詳しくは、「Desktop Lockをインストールするには」を参照してください。
- ユーザーが、ドメインに参加しているデスクトップアプライアンスや再目的化されたPCを使用する場合は、管理者権限を持つアカウントでReceiver for Windows Enterpriseをインストールします。Receiver for Windowsを構成するときに、適切なストアのXenApp ServicesサイトのURLを指定します。スマートカードを使用してデバイスにログオンして、ストアからリソースにアクセスできることを確認した後で、Citrix Desktop Lockをインストールします。詳しくは、「Desktop Lockをインストールするには」を参照してください。
- そのほかの場合は、適切なバージョンのCitrix Receiverをユーザーデバイスにインストールします。ドメインに参加しているデバイスのユーザーがXenDesktopやXenAppに接続するときのスマートカードパススルー認証を有効にするには、管理者アカウントを使ってReceiver for Windowsをコマンドラインでインストールします。このときに、/includeSSONオプションを指定します。詳しくは、「コマンドラインパラメーターを使用したReceiver for Windowsの構成とインストール」を参照してください。
  ドメインポリシーまたはローカルコンピューターポリシーで、スマートカード認証が使用されるようにReceiver for Windowsが構成されていることを確認します。ドメインポリシーは、グループポリシー管理コンソールを使用してReceiver for Windowsのグループポリシーオブジェクトのテンプレートファイルicaclient.admを、ユーザーアカウントが属しているドメインのドメインコントローラーにインポートします。デバイスごとに構成する場合は、そのデバイス上のグループポリシーオブジェクトエディターを使用してこのテンプレートを構成します。詳しくは、「グループポリシーオブジェクトテンプレートによるReceiverの構成」を参照してください。

  [Smart card authentication] ポリシーを有効にします。スマートカードの資格情報が自動的に使用（パススルー）されるようにするには、[Use pass-through authentication for PIN] チェックボックスをオンにします。さらに、XenDesktopおよびXenAppにスマートカードの資格情報がパススルーされるようにするには、[Local user name and password] ポリシーを有効にして、[Allow pass-through authentication for all ICA connections] チェックボックスをオンにします。詳しくは、「ICA Settings Reference」を参照してください。

  ドメインに参加しているデバイスのユーザーがXenDesktopやXenAppに接続するときのスマートカードパススルー認証を有効にした場合は、ストアのURLをInternet Explorerのローカルイントラネットまたは信頼済みサイトのゾーンに追加します。この場合、そのゾーンのセキュリティ設定で [現在のユーザー名とパスワードで自動的にログオンする] が選択されて

いることを確認してください。

- 必要な場合は、ストア（内部ネットワーク上のユーザーの場合）やNetScaler Gatewayアプライアンス（リモートユーザーの場合）に接続するための詳細を適切な方法でユーザーに提供します。構成情報のユーザーへの提供について詳しくは、「Citrix Receiver」を参照してください。

ドメインに参加しているユーザーデバイスにReceiver for Windowsをインストールするときに、パススルー認証（シングルサインオン）を有効にできます。XenDesktopおよびXenAppによってホストされているデスクトップおよびアプリケーションにアクセスするときにスマートカードの資格情報が自動的に使用（パススルー）されるようにするには、ストアのdefault.storeフロント用のデフォルトの.icaファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってストアのdefault テキストエディターを使ってストアのicaファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storename\App_Data\フォルダーにあります。ここで、storenameはストアの作成時に指定した名前です。
2. NetScaler Gatewayを使用しないでストアにアクセスするユーザーのスマートカード資格情報のパススルーを有効にするには、次の設定を[Application]セクションに追加します。
   DisableCtrlAltDel=Off
   この設定はストアのすべてのユーザーに適用されます。デスクトップおよびアプリケーションに対するドメインパススルー認証とスマートカードパススルー認証の両方を有効にするには、これらの認証方法について個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。
3. NetScaler Gatewayを使用してストアにアクセスするユーザーのスマートカード資格情報のパススルーを有効にするには、次の設定を[Application]セクションに追加します。
   UseLocalUserAndPassword=On
   この設定はストアのすべてのユーザーに適用されます。一部のユーザーに対してのみパススルー認証を有効にする場合は、それらのユーザー用に個別のストアを作成する必要があります。この場合、どのストアにアクセスすべきかをユーザーに通知してください。

パスワードの有効期限切れ通知期間の構成

May 22, 2017

Citrix Receiver for Webサイトのユーザーがいつでもパスワードを変更できるように設定してある場合は、パスワードの有効期限切れが近いローカルユーザーがログオンしたときに警告が表示されます。デフォルトでは、ユーザーに対する通知期間は、適用されるWindowsポリシーの設定によって決まります。すべてのユーザーに対するカスタムの通知期間を設定するには、認証サービスの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、 **[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの **[認証方法の管理]** をクリックします。
3. **[認証方法の管理]** ページで、 **[ユーザー名とパスワード]** > **[設定]** ドロップダウンメニューから **[パスワードオプションの管理]** を選択し、 **[ユーザーにパスワードの変更を許可する]** チェックボックスをオンにします。
4. **[常に許可...]** を選択し、 **[パスワードの期限が切れる前にユーザーにリマインドする]** の下で項目を選択します。

注：StoreFrontでは、Active Directoryの細かい設定が可能なパスワードポリシーはサポートされません。

ストアの構成と管理

May 22, 2017

Citrix StoreFrontでは、XenAppおよびXenDesktopからアプリケーションやデスクトップをまとめるストアを作成して管理し、ユーザーにリソースに対するセルフサービスアクセスをオンデマンドで提供できます。

ストアの作成または削除	必要とするできるだけ多くの追加ストアを構成します。
認証が不要なストアの作成	追加の未認証のストアを構成し、認証不要（匿名）ユーザーのアクセスをサポートする。
ユーザー用のストアプロビジョニングファイルのエクスポート	ストアに対して構成されたNetScaler Gateway展開やビーコンなど、ストアに対する接続の詳細を含んでいるファイルを生成します。
ストアの非表示とアドバタイズ	ユーザーがメールアドレスによるアカウント検出機能または完全修飾ドメイン名（FQDN）を使ってCitrix Receiverを構成する場合、ユーザーに表示されているストアがユーザーのアカウントに追加されないようにします。
ストアに表示するリソースの管理	ストアからのリソースの追加と削除
NetScaler Gatewayを介したストアへのリモートアクセスの管理	公共のネットワークから接続するユーザーに対してNetScaler Gatewayを介したストアへのアクセスを構成します。
Citrix Onlineアプリケーションのストアへの統合	ストアに追加するCitrix Onlineアプリケーションを選択して、ユーザーがCitrix OnlineアプリケーションをサブスクライブしたときのCitrix Receiverの動作を指定します。
共通のサブスクリプションデータストアを共有する2つのStoreFrontストアの構成	共通のサブスクリプションデータベースを共有する2つのストアの構成
上級ストア設定	上級ストア設定を構成します。

Create or remove a store

May 22, 2017

Use the Create Store task to configure additional stores. You can create as many stores as you need; for example, you can create a store for a particular group of users or to group together a specific set of resources. You can also create an unauthenticated store that allows for anonymous, or unauthenticated store. To create this type of store, refer to the Create an unauthenticated store instruction.

To create a store, you identify and configure communications with the servers providing the resources that you want to make available in the store. Then, optionally, you configure remote access to the store through NetScaler Gateway.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click Create Store.
3. On the Store Name page, specify a name for your store and click Next.
   Store names appear in Citrix Receiver under users' accounts, so choose a name that gives users information about the content of the store.
4. On the Delivery Controllers page, list the infrastructure providing the resources that you want to make available in the store. Click Add.
5. In the Add Delivery Controller dialog box, specify a name that will help you to identify the deployment and indicate whether the resources that you want to make available in the store are provided by XenDesktop, XenApp, or AppController. For App Controller deployments, ensure that the name you specify does not contain any spaces.
6. If you are adding details of XenDesktop or XenApp servers, continue to Step 7. To make applications managed by App Controller available in the store, enter the name or IP address of an App Controller virtual appliance in the Server box and specify the port for StoreFront to use for connections to App Controller. The default port is 443. Continue to Step 11.
7. To make desktops and applications provided by XenDesktop or XenApp available in the store, add the names or IP addresses of your servers to the Servers list. Specify multiple servers to enable fault tolerance, listing the entries in order of priority to set the failover sequence. For XenDesktop sites, give details of Delivery Controllers. In the case of XenApp farms, list servers running the Citrix XML Service.
8. Select from the Transport type list the type of connections for StoreFront to use for communications with the servers.
   - To send data over unencrypted connections, select HTTP. If you select this option, you must make your own arrangements to secure connections between StoreFront and your servers.
   - To send data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), select HTTPS. If you select this option for XenDesktop and XenApp servers, ensure that the Citrix XML Service is set to share its port with Microsoft Internet Information Services (IIS) and that IIS is configured to support HTTPS.
   - To send data over secure connections to XenApp servers using the SSL Relay to perform host authentication and data encryption, select SSL Relay.

   Note: If you are using HTTPS or the SSL Relay to secure connections between StoreFront and your servers, ensure that the names you specify in the Servers list match exactly (including the case) the names on the certificates for those servers.

9. Specify the port for StoreFront to use for connections to the servers. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. In the case of XenDesktop and XenApp servers, the specified port must be the port used by the Citrix XML Service.
10. If you are using the SSL Relay to secure connections between StoreFront and XenApp servers, specify the TCP port of the SSL Relay in the SSL Relay port box. The default port is 443. Ensure that all the servers running the SSL Relay are configured to monitor the same port.
11. Click OK. You can configure stores to provide resources from any mixture of XenDesktop, XenApp, and App Controller deployments. Repeat Steps 4 to 11, as necessary, to list additional deployments providing resources for the store. When you have added all the required resources to the store, click Next.
12. On the Remote Access page, specify whether and how users connecting from public networks can access the store through NetScaler Gateway.
    - To make the store unavailable to users on public networks, make sure you do not check **Enable Remote Access**. Only local users on the internal network will be able to access the store.
    - To enable remote access, check **Enable Remote Access**.
      - To make only resources delivered through the store available through NetScaler Gateway, select No VPN tunnel. Users log on directly to NetScaler Gateway and do not need to use the NetScaler Gateway Plug-in.
      - To make the store and all other resources on the internal network available through an SSL virtual private network (VPN) tunnel, select Full VPN tunnel. Users require the NetScaler Gateway Plug-in to establish the VPN tunnel.

    If it is not already enabled, the pass-through from NetScaler Gateway authentication method is automatically enabled when you configure remote access to the store. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.

13. If you enabled remote access, continue to the next procedure to specify the NetScaler Gateway deployments through which users can access the store. Otherwise, on the Remote Access page, click Create. Once the store has been created, click Finish.

Complete the following steps to configure remote access through NetScaler Gateway to the store that you created in the previous procedure. It is assumed that you have completed all the preceding steps.

1. On the **Remote Access** page of the **Create Store** wizard, select from the **NetScaler Gateway appliances** list the deployments through which users can access the store. Any deployments you configured previously for other stores are available for selection in the list. If you want to add a further deployment to the list, click Add. Otherwise, continue to Step 12.
2. On the **Add NetScaler Gateway Appliance General Settings** page, specify a name for the NetScaler Gateway deployment that will help users to identify it.
   Users see the display name you specify in Citrix Receiver, so include relevant information in the name to help users decide whether to use that deployment. For example, you can include the geographical location in the display names for your NetScaler Gateway deployments so that users can easily identify the most convenient deployment for their location.

3. Enter the URL of the virtual server or user logon point for your deployment. Specify the product version used in your deployment.
   The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the NetScaler Gateway virtual server FQDN. Using the same FQDN for StoreFront and the NetScaler Gateway virtual server is not supported.

4. Select the usage of the NetScaler Gateway from the available options.
   + **Authentication and HDX routing:** The NetScaler Gateway will be used for Authentication, as well as for routing

any HDX sessions.
+ **Authentication Only:** The NetScaler Gateway will be used for Authentication and not for any HDX session routings.
+ **HDX routing Only:** The NetScaler Gateway will be used for HDX session routings and not for Authentication.

5. On the Secure Ticket Authority (STA) page, if you are making resources provided by XenDesktop or XenApp available in the store, list all the Secure Ticket Authority page URLs for servers running the STA. Add URLs for multiple STAs to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

   The STA is hosted on XenDesktop and XenApp servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.
6. Choose to set the Secure Ticket Authority to be load balanced. You can also specify the time interval after which the non-responding STAs are bypassed.
7. If you want XenDesktop and XenApp to keep disconnected sessions open while Citrix Receiver attempts to reconnect automatically, select the **Enable session reliability** check box. If you configured multiple STAs and want to ensure that session reliability is always available, select the **Request tickets from two STAs**, where available check box. StoreFront obtains session tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If, for any reason, StoreFront is unable to contact two STAs, it falls back to using a single STA.
8. On Authentication Settings page, select the version of NetScaler gateway you want to configure.
9. Specify the VServer IP address of the NetScaler Gateway appliance, if required. A VServer IP address is required for Access Gateway 9.x appliances, but optional for more recent product versions. The VServer IP address is the IP address that NetScaler Gateway uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the NetScaler Gateway appliance. Where specified, StoreFront uses the VServer IP address to verify that incoming requests originate from a trusted device.
10. Select from the Logon type list the authentication method you configured on the appliance for Citrix Receiver users. The information you provide about the configuration of your NetScaler Gateway appliance is added to the provisioning file for the store. This enables Citrix Receiver to send the appropriate connection request when contacting the appliance for the first time.

    - If users are required to enter their Microsoft Active Directory domain credentials, select Domain.
    - If users are required to enter a tokencode obtained from a security token, select Security token.
    - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select Domain and security token.
    - If users are required to enter a one-time password sent by text message, select SMS authentication.
    - If users are required to present a smart card and enter a PIN, select Smart card.

    If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from theSmart card fallback list.

11. Enter the NetScaler Gateway authentication service URL in the Callback URL box. This is an optional field. StoreFront automatically appends the standard portion of the URL. Enter the internally accessible URL of the appliance. StoreFront contacts the NetScaler Gateway authentication service to verify that requests received from NetScaler Gateway originate from that appliance.
12. Click Create to add your NetScaler Gateway deployment to the list on the Remote Access page. Repeat Steps 1 to 11, as necessary, to add more NetScaler Gateway deployments to the NetScaler Gateway appliances list. If you enable access through multiple deployments by selecting more than one entry in the list, specify the default deployment to be used to access the store.

13. On the Remote Access page, click Create. Once the store has been created, click Finish.

Your store is now available for users to access with Citrix Receiver, which must be configured with access details for the store. There are a number of ways in which you can provide these details to users to make the configuration process easier for them. For more information, see User access options.

Alternatively, users can access the store through the Receiver for Web site, which enables users to access their desktops and applications through a webpage. The URL for users to access the Receiver for Web site for the new store is displayed when you create the store.

When you create a new store, the XenApp Services URL is enabled by default. Users of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with users who have older Citrix clients that cannot be upgraded, can access stores directly using the XenApp Services URL for the store. The XenApp Services URL has the form http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, where serveraddress is the FQDN of the server or load balancing environment for your StoreFront deployment and storename is the name you specified for the store in Step 3.

Create a store for single server deployments on a nondomain-joined server

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Create Store**.
3. On the **Store Name** page, specify a name for your store and click **Next**.
   Store names appear in Citrix Receiver under users' accounts, so choose a name that gives users information about the content of the store.

4. On the **Delivery Controllers** page, list the infrastructure providing the resources that you want to make available in the store. Click **Add**.
5. In the **Add Delivery Controller** dialog box, specify a name that will help you to identify the deployment and indicate whether the resources that you want to make available in the store are provided by XenDesktop, XenApp, or XenMobile AppController. For App Controller deployments, ensure that the name you specify does not contain any spaces.
6. If you are adding details of XenDesktop or XenApp servers, continue to Step 7. To make applications managed by App Controller available in the store, enter the name or IP address of an App Controller virtual appliance in the Server box and specify the port for StoreFront to use for connections to App Controller. The default port is 443. Continue to Step 11.
7. To make desktops and applications provided by XenDesktop or XenApp available in the store, add the name or IP address of your server to the **Servers** box. For XenDesktop sites, give details of Delivery Controllers. In the case of XenApp farms, list the server running the Citrix XML Service.
8. Select from the **Transport type** list the type of connections for StoreFront to use for communications with the server.
   - To send data over unencrypted connections, select HTTP. If you select this option, you must make your own arrangements to secure connections between StoreFront and your server.
   - To send data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), select HTTPS. If you select this option for XenDesktop and XenApp servers, ensure that the Citrix XML Service is set to share its port with Microsoft Internet Information Services (IIS) and that IIS is configured to support HTTPS.
   - To send data over secure connections to XenApp servers using the SSL Relay to perform host authentication and data encryption, select SSL Relay.

     Note: If you are using HTTPS or the SSL Relay to secure connections between StoreFront and your server, ensure that the name you specify in the **Servers** box matches exactly (including the case) the name on the certificate for that server.

9. Specify the port for StoreFront to use for connections to the server. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. In the case of XenDesktop and XenApp servers, the specified port must be the port used by the Citrix XML Service.
10. If you are using the SSL Relay to secure connections between StoreFront and the XenApp server, specify the TCP port of the SSL Relay in the SSL Relay port box. The default port is 443. Ensure that all the servers running the SSL Relay are configured to monitor the same port.
11. Click **OK**. You can configure stores to provide resources from any mixture of XenDesktop, XenApp, and App Controller deployments. Repeat Steps 4 to 11, as necessary, to list additional deployments providing resources for the store. When you have added all the required resources to the store, click Next.
12. On the **Remote Access** page, specify whether and how users connecting from public networks can access the store through NetScaler Gateway.
    - To make the store unavailable to users on public networks, select **None**. Only local users on the internal network will be able to access the store.
    - To make only resources delivered through the store available through NetScaler Gateway, select **No VPN tunnel**. Users log on directly to NetScaler Gateway and do not need to use the NetScaler Gateway Plug-in.
    - To make the store and all other resources on the internal network available through an SSL virtual private network (VPN) tunnel, select **Full VPN tunnel**. Users require the NetScaler Gateway Plug-in to establish the VPN tunnel.

      If it is not already enabled, the pass-through from NetScaler Gateway authentication method is automatically enabled when you configure remote access to the store. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.
13. If you enabled remote access, continue to Provide remote access to the store through NetScaler Gateway to specify the NetScaler Gateway deployments through which users can access the store. Otherwise, on the **Remote Access** page, click **Next**.
14. On the **Configure Authentication Methods** page, select the methods by which users will authenticate and access resources, and click **Next**.
15. On the **Configure Password Validation** page, select the delivery controllers to provide the password validation, click **Next**.
16. On the **XenApp Services URL** page, configure the URL for users who us PNAgent to access application and desktops and click **Create**.

Server Group Node in the left and **Action** panes is replaced by **Change Base URL**. The only option available is to change the base URL, because server groups are not available in nondomain-joined servers.

Remove a store

Use the Remove Store task to delete a store. When you remove a store, any associated Receiver for Web sites, Desktop Appliance sites, and XenApp Services URLs are also deleted.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

認証が不要なストアの作成

May 22, 2017

認証不要（匿名）ユーザーのアクセスをサポートする、認証が不要なストアを追加で構成するには、[ストアの作成] タスクを使用します。このストアは必要なだけ作成できます。たとえば、特定のユーザーグループ用にストアを作成したり、特定のリソースセットを集約するストアを作成したりできます。

認証不要なストアでは、NetScaler Gatewayを介したリモートアクセスは許可されません。

認証不要なストアを作成するには、そのストアのユーザーにリソースを提供するサーバーを指定して、その通信構成を行います。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで [ストア］ノードを選択して、［操作］ペインの［ストアの作成］をクリックします。
3. ［ストア名］ページで、ストアの名前を指定して、**[このストアへのアクセスを非認証 (匿名) ユーザーにのみ許可する]** を選択し、［次へ］をクリックします。
   ストアの名前はCitrix Receiverでユーザーアカウントの下に表示されるため、ユーザーにとってわかりやすい名前を指定してください。
4. **[Delivery** Controller］ページでは、リソースを提供するインフラストラクチャを一覧に追加します。[Add］をクリックします。
5. ［Delivery Controllerの追加］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、ストアで使用できるようにするリソースが［XenApp］または［AppController］で提供されるかどうかを指定します。XenMobile（App Controller）を選択する場合は、表示名として入力した文字列にスペースが含まれていないことを確認してください。Controllerを追加するときは、匿名アプリ機能をサポートしていることを確認してください。匿名アプリ機能をサポートしないControllerで認証不要なストアを構成すると、ストアから匿名アプリを使用できなくなります。
6. XenAppサーバーの詳細を追加している場合は、手順7.に進みます。App Controllerにより管理されるアプリケーションをストアで使用できるようにするには、XenMobile（App Controller）仮想アプライアンスの名前またはXenMobile（App Controller）アドレスを［サーバー］ボックスに入力し、XenMobile（App Controller）への接続に使用するIPのポートを指定します。デフォルトのTCPポートは443です。手順10.に進みます。
7. リソースを提供するインフラストラクチャの種類としてXenAppを選択した場合は、サーバーの名前またはIPアドレスを［サーバー］一覧に追加します。この一覧に複数のサーバーを追加すると、その順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。
8. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには [HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。

   注：StoreFrontとサーバーの間の通信をHTTPSで保護する場合は、［サーバー］ボックスの一覧に指定したサーバー名が

そのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。

9. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用されるポート番号を指定する必要があります。
10. ［OK］をクリックします。XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順4.～12.を繰り返し、ストアにリソースを提供する展開環境を一覧に追加します。必要なリソースをすべてストアに追加したら、［作成］をクリックします。

これで認証不要なストアが作成されました。このストアにユーザーがアクセスできるようにするには、Citrix Receiverでアクセス情報を構成する必要があります。ユーザーによるReceiverの構成プロセスを簡単にするために、いくつかの方法が用意されています。詳しくは、「ユーザーアクセスオプション」を参照してください。
また、Receiver for Webサイトを使用すると、ユーザーがWebページからデスクトップやアプリケーションにアクセスできるようになります。認証が不要なストアのデフォルトでは、Receiver for Webにアプリケーションがフォルダー階層で表示されるようになり、フォルダーパスの情報も表示されます。新しいストアにアクセスするためのReceiver for WebサイトのURLは、ストアを作成するときに表示されます。

デフォルトでは、新しいストアを作成するときに、XenApp ServicesサイトのURLが有効になります。ドメインに参加していないデスクトップアプライアンスのユーザー、Citrix Desktop Lockを実行している再目的化されたPCのユーザー、およびアップグレードできない古いバージョンのCitrixクライアントのユーザーは、XenApp Servicesサイトから直接そのストアに接続できます。XenApp Services URLの形式は、http[s]://serveraddress/Citrix/storename/PNAgent/config.xmlの形式です。ここで、serveraddressはStoreFront展開環境のサーバーまたは負荷分散環境の完全修飾ドメイン名で、storenameは上記手順3で指定した名前です。

注：web.configファイルでパラメーター LogoffAction=”terminate"を構成しても、認証不要なストアにアクセスするCitirx Receiver for Webセッションは終了しません。このweb.configファイルは、通常C:\inetpub\wwwroot\Citrix\storename\フォルダーにあります（storenameはストア作成時に指定したストア名）。これらのセッションが正しく終了するようにするには、ストアのXenAppサーバーで［XML要求を信頼する］オプションが有効になっている必要があります（XenAppおよびXenDesktopドキュメントの「*Citrix XML Serviceのポートと信頼を設定する*」を参照）。

ユーザー用のストアプロビジョニングファイルのエクスポート

May 22, 2017

ストアで使用されるNetScaler Gateway環境やビーコンポイントなどの詳細情報が定義されたプロビジョニングファイルを生成するには、［複数ストアのプロビジョニングファイルのエクスポート］および［プロビジョニングファイルのエクスポート］タスクを使用します。ユーザーにプロビジョニングを提供すると、ユーザーがCitrix Receiverを簡単に構成できるようになります。Citrix Receiverプロビジョニングファイルは、Receiver for Webサイトから入手できるようにすることもできます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。Citrix StoreFront管理コンソールの左ペインで、［ストア］ノードを選択します。
2. 複数のストアの詳細情報が定義されたプロビジョニングファイルを生成するには、［操作］ペインの［複数ストアのプロビジョニングファイルのエクスポート］をクリックして、対象のサイトを選択します。
3. ［エクスポート］をクリックして、拡張子が.crのプロビジョニングファイルをネットワーク上の適切な場所に保存します。

ユーザーに対するストアの非表示および提供

May 22, 2017

ユーザーがメールアドレスによるアカウント検出機能または完全修飾ドメイン名（FQDN）を使ってCitrix Receiverを構成する場合、特定のストアがユーザーのアカウントに追加されないように、そのストアを非表示に設定できます。これを行うには、［ストアを表示しない］タスクを使用します。新規に作成するストアのデフォルトでは、ユーザーがCitrix ReceiverでStoreFrontストアを追加するときに、オプションとしてそのストアが表示されます。ストアを非表示にしても、ユーザーがストアにアクセスできなくなるわけではありません。ユーザーは、メールアドレスによるアカウント検出機能の代わりにCitrix Receiverでのストア接続を手作業で構成したり、セットアップURLやプロビジョニングファイルを使用したりする必要があります。ストアの非表示状態を解除するには、［ストアのアドバタイズ］タスクを使用します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで［ストア設定の構成］>［ストアのアドバタイズ］の順にクリックします。
3. ［ストアのアドバタイズ］ページで［ストアのアドバタイズ］または［ストアの非表示］を選択します。

ストアに表示するリソースの管理

May 22, 2017

XenDesktop、XenApp、およびApp Controllerによって提供されたストアリソースから追加または削除したり、これらのリソースを提供するサーバーの詳細を変更したりするには、［Controllerの管理］タスクを使用します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインの［Delivery Controllerの管理］をクリックします。
3. ストアにデスクトップやアプリケーションを提供するXenDesktop、XenApp、またはApp Controller展開環境を追加するには、［Delivery Controllerの管理］ダイアログボックスで［追加］をクリックします。展開環境の設定を変更するには、［Delivery Controller］ボックスの一覧でエントリを選択して［編集］をクリックします。展開環境により提供されるリソースをストアから削除するには、ボックスの一覧でエントリを選択して［削除］をクリックします。
4. ［Controllerの追加］または［Controllerの編集］ダイアログボックスで、この展開環境に対するわかりやすい名前を指定し、リソースを提供するインフラストラクチャの種類（［XenDesktop］、［XenApp］、または［AppController］）を選択します。App Controllerを選択する場合は、表示名として入力した文字列にスペースが含まれていないことを確認してください。
5. インフラストラクチャの種類としてXenDesktopまたはXenAppサーバーを選択した場合は、手順7.に進みます。App Controllerにより管理されるアプリケーションをストアで使用できるようにするには、App Controller仮想アプライアンスの名前またはIPアドレスを［サーバー］ボックスに入力し、App Controllerへの接続に使用するStoreFrontのポートを指定します。デフォルトのTCPポートは443です。手順10.に進みます。
6. XenDesktopまたはXenAppが提供するデスクトップやアプリケーションをストアに追加するには、［追加］をクリックしてサーバーの名前またはIPアドレスを入力します。複数のサーバーを指定すると、web.configファイルの構成に基づいて負荷分散またはフェールオーバーが有効になります。デフォルトでは、負荷分散が構成されています。フェールオーバーを構成すると、サーバーの一覧の順番に基づいてフェールオーバーされます。XenDesktopサイトの場合は、Delivery Controllerの詳細を指定します。XenAppファームの場合は、Citrix XML Serviceを実行しているサーバーを一覧に追加します。サーバーの名前またはIPアドレスを変更するには、［サーバー］ボックスの一覧でエントリを選択して［編集］をクリックします。一覧からエントリを削除するには、そのエントリを選択して［削除］をクリックします。これにより、そのサーバーからのリソースがストアに列挙されなくなります。
7. ［トランスポートの種類］ボックスの一覧から、StoreFrontでサーバーとの通信に使用する接続の種類を選択します。
   - 暗号化されていない接続でデータを送信するには［HTTP］を選択します。このオプションを選択する場合は、StoreFrontとサーバー間の接続を何らかの方法で保護することを検討してください。
   - SSL（Secure Sockets Layer）またはTLS（Transport Layer Security）を使用する保護されたHTTP接続でデータを送信するには、［HTTPS］を選択します。XenDesktopまたはXenAppサーバーに対してこのオプションを選択する場合は、Citrix XML ServiceがポートをIIS（Microsoftインターネットインフォメーションサービス）と共有する設定になっていることと、IISがHTTPSをサポートするように構成されていることを確認してください。
   - XenAppサーバーとの通信でSSL Relayによるホスト認証とデータの暗号化を実行するには、［SSL Relay］を選択します。

   注：StoreFrontとサーバーの間の通信でHTTPSまたはSSL Relayを使用する場合は、［サーバー］ボックスの一覧に指定したサーバー名がそのサーバーの証明書のサーバー名と一致することを確認してください（大文字/小文字は区別されます）。
8. StoreFrontがサーバーに接続するときに使用するポートを指定します。デフォルトでは、HTTP接続およびSSL Relay接続では80、HTTPS接続では443が使用されます。XenDesktopおよびXenAppサーバーの場合、Citrix XML Serviceで使用され

るポート番号を指定する必要があります。

9. StoreFrontとXenAppサーバーの間の接続をSSL Relayで保護する場合は、SSL RelayのTCPポートを［SSL Relayポート］ボックスで指定します。デフォルトのTCPポートは443です。SSL Relayを実行するすべてのサーバーで同じポートが構成されていることを確認してください。
10. ［OK］をクリックします。XenDesktop、XenApp、およびApp Controllerの展開環境を自由に組み合わせてストアを作成できます。必要に応じて手順3.～10.を繰り返し、［Delivery Controller］の一覧にほかの展開環境を追加したり既存のエントリを変更したりします。

NetScaler Gatewayを介したストアへのリモートアクセスの管理

May 22, 2017

公共のネットワークから接続するユーザーに対してNetScaler Gatewayを介したストアへのアクセスを構成するには、[リモートアクセス設定]タスクを使用します。認証不要なストアでは、NetScaler Gatewayを介したリモートアクセスは許可されません。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで［リモートアクセス設定の**構成**］**をクリックします。**
3. ［リモートアクセス設定の**構成**］ダイアログボックスでは、公共のネットワーク上のユーザーにNetScaler Gatewayを介したアクセスを提供するかどうか、およびその方法を指定します。
   - 公共のネットワーク上でストアをユーザーが使用できないようにするには、**[リモートアクセスの有効化]** チェックボックスをオフにします。これにより、内部ネットワークのローカルユーザーのみがストアにアクセスできるようになります。
   - リモートアクセスを有効にするには、**[リモートアクセスの有効化]** をオンにします。
     - NetScaler Gateway経由でアクセスするユーザーにストアのリソースのみを提供するには、[VPNトンネルなし]を選択します。この場合、ユーザーはNetScaler Gatewayに直接ログオンするため、NetScaler Gateway Plug-inを使用する必要はありません。
     - SSL（Secure Sockets Layer）仮想プライベートネットワーク（VPN）トンネルを介して内部ネットワーク上のストアやほかのリソースへのアクセスを提供するには、［完全VPNトンネル］を選択します。この場合、ユーザーはVPNトンネルを確立するためのNetScaler Gateway Plug-inを使用する必要があります。

   ストアへのリモートアクセスを有効にすると、認証方法としてNetScaler Gatewayからのパススルーが自動的に有効になります。ユーザーはNetScaler Gatewayにログオンするときに認証されるため、ストアにアクセスするときは自動的にログオンできます。

4. リモートアクセスを有効にした場合は、ユーザーがストアにアクセスするときに使用する展開環境を[NetScaler Gatewayアプライアンス]一覧から選択します。この一覧には、このストアやほかのストアの作成時に追加したゲートウェイ環境が表示されます。一覧にゲートウェイ環境を追加する場合は、［追加］をクリックします。追加しない場合は、手順26.に進みます。
5. ［全般設定］ページで、NetScaler Gateway展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。
6. 展開環境の仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。
7. 展開環境でAccess Gateway 5.0が実行されている場合は、手順9.に進みます。それ以外の場合は、必要に応じてNetScaler

GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

8. NetScaler Gateway 11、NetScaler Gateway 10.1、Access Gateway 10、またはAccess Gateway 9.3のアプライアンスを追加する場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
   - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
   - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
   - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

   スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。手順10.に進みます。

9. Access Gateway 5.0のアプライアンスを追加する場合は、ユーザーのログオンポイントのホスト（スタンドアロンのアプライアンスまたはクラスターの一部であるAccess Controllerサーバー）を指定します。クラスターを追加する場合は、［次へ］をクリックして手順11.に進みます。
10. NetScaler Gateway 11、NetScaler Gateway 10.1、Access Gateway 10、Access Gateway 9.3、またはスタンドアロンAccess Gateway 5.0アプライアンスを追加する場合は、［コールバックURL］ボックスにNetScaler Gateway認証サービスのURLを入力します。URLの標準的な部分は自動的に補完されます。［次へ］をクリックして手順13.に進みます。
アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

11. StoreFrontにAccess Gateway 5.0クラスターを追加する場合は、［アプライアンス］ページでクラスター内のアプライアンスのIPアドレスまたはFQDNを一覧に追加して、［次へ］をクリックします。
12. ［サイレント認証を有効にする］ページで、Access Controllerサーバーで実行されている認証サービスのURLを一覧に追加します。一覧に複数のサーバーのURLを追加すると、その順番に基づいてフェールオーバーされます。［Next］をクリックします。
StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

13. すべての展開環境で、XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、［Secure Ticket Authority（STA）］ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

14. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。

［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

15. ［作成］をクリックします。これにより、［リモートアクセス設定］ダイアログボックスの一覧にNetScaler Gatewayの展開環境が追加されます。
16. 必要に応じて手順4.～15.を繰り返し、［NetScaler Gatewayアプライアンス］の一覧にNetScaler Gatewayの展開環境を追加します。一覧で複数のエントリを選択して複数のゲートウェイ環境を介したアクセスを有効にする場合は、デフォルトで使用されるアプライアンスを選択します。

Citrix Onlineアプリケーションをストアに統合する

May 22, 2017

［Citrix Online統合］タスクを使用すると、ストアにCitrix Onlineアプリケーションを追加して、ユーザーがそれらのCitrix Onlineアプリケーションをサブスクライブしたときの Citrix Receiverの動作を指定できます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでストアを選択します。［操作］ペインで、**［ストア設定の構成］**＞［Citrix Onlineとの統合］の順にクリックします。
3. ストアに追加するCitrix Onlineアプリケーションを選択して、ユーザーがCitrix Onlineアプリケーションをサブスクライブしたときの Citrix Receiverの動作を指定します。
   - 選択したアプリケーションの試用アカウントをユーザーがセットアップできるようにするには、［ユーザーのトライアルアカウントのセットアップを必要に応じて支援する］を選択します。
   - 選択したアプリケーションのアカウントを取得するためにシステム管理者に問い合わせるように指示するメッセージをユーザーに表示するには、［ユーザーがヘルプデスクにアカウントについて問い合わせるようにする]を選択します。
   - 選択したアプリケーションのアカウントをすべてのユーザーが持っている場合は、［アプリケーションを直ちに追加する］を選択します。

Configure two StoreFront stores to share a common subscription datastore

May 22, 2017

As of version 2.0, StoreFront no longer uses an SQL database to maintain its subscription data. Citrix replaced the SQL database with a Windows datastore that requires no additional configuration when StoreFront is first installed. The installation installs the Windows datastore locally on each StoreFront server. In StoreFront server group environments, each server also maintains a copy of the subscription data used by its store. This data is propagated to other servers to maintain user subscriptions across the whole group. By default, StoreFront creates a single datastore for each store. Each subscription datastore is updated independently from each other store.

Where different configuration settings are required, it is common for administrators to configure StoreFront with two distinct stores; one for external access to resources using Netscaler Gateway and another for internal access using the corporate LAN. You can configure both "external" and "internal" stores to share a common subscription datastore by making a simple change to the store web.config file.

In the default scenario involving two stores and their corresponding subscription datastores, a user must subscribe to the same resource twice. Configuring the two stores to share a common subscription database improves and simplifies the roaming experience when users access the same resource from inside or outside the corporate network. With a shared subscription datastore it does not matter whether they use the "external" or "internal" store when they initially subscribe to a new resource.

- Each store has a web.config file located in C:\inetpub\wwwroot\citrix\<storename>.
- Each store web.config contains a client endpoint for the Subscription Store Service.

<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<StoreName>" authenticationMode="windows" transferMode="Streamed">

The subscription data for each Store is located in:

C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>

For two stores to share a subscription datastore, you need only point one store to the subscription service end point of the other store. In the case of a server group deployment, all servers have identical pairs of stores defined and identical copies of the shared datastore they both share.

Note: The XenApp, XenDesktop and AppC controllers configured on each store must match exactly; otherwise, an inconsistent set of resource subscriptions on one store compared to another might occur. Sharing a datastore is supported only when the two stores reside on the same StoreFront server or server group deployment.

StoreFront subscription datastore endpoints

1. On a single StoreFront deployment, open the external store web.config file using Notepad and search for the clientEndpoint. For example:
   <subscriptionsStoreClient enabled="true">
   <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_External" authenticationMode="windows" transferMode="Streamed">
   <clientCertificate thumbprint="0" />
   </clientEndpoint>
   </subscriptionsStoreClient>
2. Change the external to match the internal store endpoint:
   <subscriptionsStoreClient enabled="true">
   <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_Internal" authenticationMode="windows" transferMode="Streamed">
   <clientCertificate thumbprint="0" />
   </clientEndpoint>
   </subscriptionsStoreClient>
3. If using StoreFront server group then propagate any changes made to the web.config file of the primary node to all other nodes.

Both stores are now set to share the internal store subscription datastore.

上級ストア設定

May 22, 2017

［ストア設定の構成］の［詳細な設定］ページを使って、詳細ストアのプロパティを構成できます。

アドレス解決の種類

フォントスムージングを許可する

セッションの再接続を許可する

特殊なフォルダーのリダイレクトを許可する

バックグラウンドヘルスチェックポーリング期間

通信のタイムアウト期間

接続タイムアウト

拡張列挙機能を有効にする

ソケットプール機能の有効化

リソースを除外キーワードでフィルターする

リソースを包含キーワードでフィルターする

リソースを種類でフィルターする

同時列挙の最大数

同時列挙の最小ファーム数

ICAクライアント名を上書きする

トークンの整合性を要求する

サーバー通信試行回数

古いクライアントでDesktop Viewerを表示する

> **Important**
>
> 複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択し、真ん中のペインでストアを選択して、［操作］

ペインで **[ストア設定の構成]** を選択します。

3. **[ストア設定の構成]** ページで **[詳細な設定]** を選択して、構成する詳細オプションを選択し、必要な変更を加えて［**OK**］をクリックします。

[詳細な設定] タスクを使って、サーバーからの要求のアドレスの種類を指定します。デフォルトは［DnsPort］です。**[詳細な設定]** の **[アドレス解決の種類]** ドロップダウンメニューから、以下のいずれかを選択します。

- DNS
- DnsPort
- IPV4
- IPV4Port
- ドット
- DotPort
- Uri
- 0 = 変更なし

HDXセッションでフォントスムージングを行うかどうかを指定できます。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[フォントスムージングを許可する]** チェックボックスをチェックし、 **[OK]** をクリックします。

HDXセッションが再接続されるようにするかどうかを指定できます。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[セッションの再接続を許可する]** チェックボックスをチェックし、 **[OK]** をクリックしてセッションの再接続を有効にします。

[詳細な設定] タスクを使ってユーザーフォルダーのリダイレクトを有効または無効にします。ユーザーフォルダーのリダイレクト機能により、サーバー上のWindowsの特殊フォルダーがローカルコンピューター上のフォルダーにマップされます。ユーザーフォルダーという用語は、［ドキュメント］、［デスクトップ］など、ユーザー固有のWindowsフォルダー（特殊フォルダー）を指すもので、Windowsのバージョンが異なっていても同様のフォルダーが存在します。

[詳細な設定] タスクを使用して、 **[特殊なフォルダーのリダイレクトを許可する]** チェックボックスをオンまたはオフにして特殊なフォルダーのリダイレクトを有効または無効にし、 **[OK]** をクリックします。

StoreFrontは、各XenDesktopブローカーやXenAppサーバー上で定期的にヘルスチェックを実行し、断続的なサーバー可用性のインパクトを減少させます。デフォルトは1分毎（00:01:00）です。［詳細な設定］タスクを使用して、 **[バックグラウンドヘルスチェックポーリング期間]** の時間を指定し、 **[OK]** をクリックしてヘルスチェックの頻度を制御します。

デフォルトでは、ストアにリソースを提供するサーバーへのStoreFrontからの要求は、30秒でタイムアウトします。通信の試行が1回失敗すると、サーバーが使用できないとみなされます。 **[詳細な設定]** タスクを使用して、デフォルトの時間に変

更を行い、 **[OK]** をクリックしてこれらの設定を変更します。

Delivery Controllerで最初の接続を確立するときに待機する秒数を指定できます。デフォルトは6です。

[詳細な設定] タスクを使用して、最初の接続を確立するときに待機する秒数を指定して **[OK]** をクリックします。

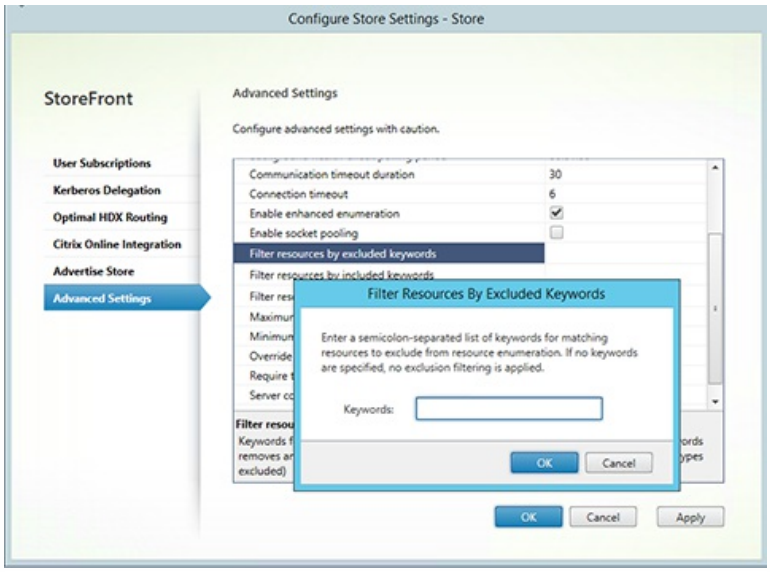
Delivery Controllerで、並列通信を有効（無効）にすることができます。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[拡張列挙機能を有効にする]** チェックボックスをオン（オフ）にし、 **[OK]** をクリックします。

ストアのソケットプール機能はデフォルトでは無効になっています。ソケットプール機能を有効にすると、StoreFrontでソケットのプールが保持されます。これにより、必要になるたびにソケットを作成して接続が閉じたときにオペレーティングシステムに戻すという処理が不要になります。この機能を有効にすると、特にSSL（Secure Sockets Layer）接続でパフォーマンスが向上します。ソケットプール機能を有効にするには、ストアの構成ファイルを編集します。 **[詳細な設定]** タスクを使用し **[ソケットプール機能を有効にする]** チェックボックスをオンにして、 **[OK]** をクリックしてソケットプール機能を有効にします。

一致するリソースを、除外キーワードでフィルターできます。除外キーワードを指定すると、それまで構成されていた包含キーワードは削除されます。既定値：［フィルターなし］（どのリソースの種類も除外されません）。

[詳細な設定] タスクを使用して、 **[リソースを除外キーワードでフィルターする]** を選択し、その右側をクリックして、セミコロンで区切ったキーワードをキーワード入力用ボックスに入力してから **[OK]** をクリックします。



一致するリソースを、包含キーワードでフィルターできます。包含キーワードを指定すると、それまで構成されていた除外キーワードは削除されます。既定値：［フィルターなし］（どのリソースの種類も除外されません）。

[詳細な設定] タスクを使用して、 **[リソースを包含キーワードでフィルターする]** を選択し、その右側をクリックして、セミコロンで区切ったキーワードをキーワード入力用ボックスに入力してから **[OK]** をクリックします。

リソースの列挙に含めるリソースの種類を選択します。既定値：［フィルターなし］（すべてのリソースの種類が含まれます）。

[詳細な設定] タスクを使用して、 **[リソースを種類でフィルターする]** を選択し、その右側をクリックして、列挙に含めるリソースの種類を選択し、 **[OK]** をクリックします。

複数のDelivery Controllerに送信する同時要求の最大数を指定します。規定値は0（制限なし）です。

[詳細な設定] タスクを使用して、 **[同時列挙の最大数]** を選択し、 **[OK]** をクリックします。

並列で列挙を行うDelivery Controllerの最小数を指定します。デフォルトは、［3］です。

[詳細な設定] タスクを使用して、 **[同時列挙の最小ファーム数]** を選択し、数値を入力してから **[OK]** をクリックします。

.ica 起動ファイルのクライアント名設定を、Citrix Receiver for Webで生成されたIDで上書きします。無効にすると、Citrix Receiverによってクライアント名が指定されます。デフォルトは、［Off］です。

[詳細な設定] タスクを使用して、 **[ICAクライアント名を上書きする]** チェックボックスをオンにし、 **[OK]** をクリックします。

有効にすると、StoreFrontによって、認証に使用されるゲートウェイとストア全体のゲートウェイとの整合性が強制されます。これらの値に不整合がある場合、ユーザーは再認証を行う必要があります。Smart Accessではこのオプションを有効にする必要があります。デフォルトは［On］です。

[詳細な設定] タスクを使用して、 **[トークンの整合性を要求する]** チェックボックスをオンにし、 **[OK]** をクリックします。

Delivery Controllerが利用不可とマークされるまでの、Delivery Controllerとの通信を試行する回数を指定します。デフォルトは［1］です。

[詳細な設定] タスクを使用して、 **[サーバー通信試行回数]** を選択し、数値を入力して **[OK]** をクリックします。

ユーザーが古いクライアントからデスクトップにアクセスする際に、Citrix Desktop Viewerウィンドウおよびツールバーを表示するかどうかを指定します。デフォルトは、［Off］です。

[詳細な設定] タスクを使用して、 **[古いクライアントでDesktop Viewerを表示する]** チェックボックスをオンにし、 **[OK]** をクリックします。

Citrix Receiver for Webサイトの管理

May 22, 2017

Citrix Receiver for Webを使って、さまざまなデバイスからアプリケーション、データ、デスクトップに簡単かつ安全にアクセスできます。StoreFrontを使って、Citrix Receiver for Webに対するCitrix Receiver for Webアプリケーションを構成します。

StoreFront管理コンソールを使って、次のCitrix Receiver for Web関連タスクを実行します。

Citrix Receiver for Webサイトの作成	Citrix Receiver for Webサイトを作成し、Webページを経由してストアにアクセスできます。
Citrix Receiver for Webサイトの構成	Receiver for Webサイトの設定を変更します。
統合Receiverエクスペリエンスのサポートの構成	StoreFrontは、クラシックと統合の両方のユーザーエクスペリエンスをサポートします。新しい統合エクスペリエンスは、中央集中管理されたHTML5ユーザーエクスペリエンス。
おすすめのアプリケーションの作成および管理	特定のカテゴリに関連するまたはそれと適合するエンドユーザーに対するお勧めのアプリケーショングループを作成します。
ワークスペースコントロールの構成	ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。
Citrix Receiver for HTML5のブラウザータブ使用の構成	ユーザーがCitrix Receiver for HTML5を使用してショートカットからリソースを起動した場合、新しいタブが表示されるのではなく、既存のブラウザータブのCitrix Receiver for Webサイトが置き換わり、そこでデスクトップまたはアプリケーションが起動するように指定します。
通信のタイムアウト期間および再試行回数の構成	デフォルトでは、Citrix Receiver for Webサイトからそのストアへの要求は、3分でタイムアウトします。通信の試行が1回失敗すると、ストアが使用できないとみなされます。デフォルトの設定を変更できます。

Citrix Receiver for Webサイトの作成

May 22, 2017

ユーザーがWebページからストアにアクセスできるようにするには、［Webサイトの作成］タスクを使用してReceiver for Webサイトを追加します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、Citrix Receiver for Webサイトを作成するストアを選択し、［操作］ペインの［Receiver for Webサイトの管理］をクリックします。
3. **［追加］**をクリックして、新しいCitrix Reciver for Webサイトを作成します。［Webサイトパス］ボックスに希望するURLを指定して、**［次へ］**をクリックします。
4. Citrix Receiverエクスペリエンスを選択して、**［次へ］**をクリックします。
5. 認証方法を選択して［作成］をクリックし、サイトが作成されたら［完了］をクリックします。
   ユーザーがこのCitrix Receiver for WebサイトにアクセスするためのURLが表示されます。Citrix Receiver for Webサイトの設定の変更について詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

デフォルトでは、ユーザーがWindowsまたはMac OS Xが動作するコンピューターからReceiver for Webサイトにアクセスすると、Citrix Receiverがユーザーデバイスにインストール済みであるかどうかが判別されます。Citrix Receiverが検出されない場合は、プラットフォームに適したCitrix Receiverをダウンロードしてインストールするためのページが開きます。この動作を変更する方法については、「Citrix Receiverの検出と展開の無効化」を参照してください。

Receiver for Webサイトのデフォルト構成では、デスクトップとアプリケーションにアクセスするために、ユーザーが適切なバージョンのCitrix Receiverをインストールする必要があります。Citrix Receiver for WebサイトのReceiver for HTML5を有効にすると、Citrix Receiverをインストールできないユーザーもリソースにアクセスできるようになります。詳しくは、「Citrix Receiver for Webサイトの構成」を参照してください。

Configure Citrix Receiver for Web sites

May 26, 2017

Citrix Receiver for Web sites enable users to access stores through a webpage. The tasks below enable you to modify settings for your Citrix Receiver for Web sites. Some advanced settings can only be changed by editing the site configuration files. For more information, see Configure Citrix Receiver for Web sites using the configuration files.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

Use the Authentication Methods task to assign authentication methods for users connecting to the Citrix Receiver for Web site. This action allows you to specify a subset of authentication methods for each Receiver for Web site.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select the relevant store that you want to modify from the results pane.
3. In the Actions pane, click **Manage Receiver for Web Sites**, click **Configure**, and choose **Authentication Methods** to specify the access methods that you want to enable for your users.
   - Select the User name and password check box to enable explicit authentication. Users enter their credentials when they access their stores.
   - Select the **SAML Authentication** check box to enable integration with a SAML Identity Provider. Users authenticate to an Identity Provider and are automatically logged on when they access their stores. From the Settings drop-down menu:
     - Select **Identity Provide**r to configure the trust to the Identity Provider.
     - Select **Service Provider** to configure the trust for the Service Provider. This information is required by the Identity Provider.
   - Select the Domain pass-through check box to enable pass-through of Active Directory domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores. In order to use this option, pass-through authentication must be enabled when Citrix Receiver for Windows is installed on users' devices. Note that Domain pass-through for Citrix Receiver for Web is limited to Windows operating systems using Chrome, Firefox, Internet Explorer, and Edge.
   - Select the Smart card check box to enable smart card authentication. Users authenticate using smart cards and PINs when they access their stores.
   - Select the Pass-through from NetScaler Gateway check box to enable pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.
4. Once the authentication method has been selected, click OK.
   For more information about modifying settings for authentication methods, see Configure the authentication service.

Use the Add Shortcuts to Websites task to provide users with rapid access to desktops and applications from websites hosted on the internal network. You generate URLs for resources available through the Citrix Receiver for Web site and embed these links on your websites. Users click on a link and are redirected to the Receiver for Web site, where they log on if they have not already done so. The Receiver for Web site automatically starts the resource. In the case of applications,

users are also subscribed to the application if they have not subscribed previously.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select the site from the results pane.
3. In the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**, and choose **Website Shortcuts**.
4. Click **Add** to enter the URL for a website on which you plan to host shortcuts. URLs must be specified in the form http[s]://hostname[:port], where hostname is the fully qualified domain name of the website host and port is the port used for communication with the host if the default port for the protocol is not available. Paths to specific pages on the website are not required. To modify a URL, select the entry in the Websites list and click Edit. Select an entry in the list and click Remove to delete the URL for a website on which you no longer want to host shortcuts to resources available through the Citrix Receiver for Web site.
5. Click Get shortcuts and then click Save when you are prompted to save your configuration changes.
6. Log on to the Citrix Receiver for Web site and copy the URLs you require to your website.

By default, user sessions on Citrix Receiver for Web sites time out after 20 minutes of inactivity. When a session times out, users can continue to use any desktops or applications that are already running but must log on again to access Citrix Receiver for Web site functions such as subscribing to applications.

Use the Session Timeout task in the **Manage Receiver for Web Sites** to change the session timeout value.

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**, choose **Session Settings**. You can specify minutes and hours for **Session timeout**. The minimum value for all time intervals is 1. The maximum equates to 1 year for each time interval.

Use the **Application and Desktops view on Receiver for Web** task in the **Manage Receiver for Web Sites** to change the session timeout value.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click Manage Receiver for Web Sites, click **Configure**, and choose **Client Interface Settings**.
3. From the **Select view** and **Default view** drop-down menus, select the views you want displayed.

To enable folder view:

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Select **Advanced Settings** and check **Enable folder view**.

By default, Citrix Receiver for Web sites offer provisioning files that enable users to configure Citrix Receiver automatically for the associated store. The provisioning files contain connection details for the store that provides the resources on the site, including details of any NetScaler Gateway deployments and beacons configured for the store.

Use the **Enable Receiver configuration** task in the **Manage Receiver for Web Sites** to change the session timeout value.

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**, and choose **Client Interface Settings**.
3. Select **Enable Receiver configuration**.

Use the **Deploy Citrix Receiver** task to configure the behavior of a Citrix Receiver for Web site when a Windows or Mac OS X user without Citrix Receiver installed accesses the site. By default, Citrix Receiver for Web sites automatically attempt to determine whether Citrix Receiver is installed when accessed from computers running Windows or Mac OS X.

If Citrix Receiver cannot be detected, the user is prompted to download and install the appropriate Citrix Receiver for their platform. The default download location is the Citrix website, but you can also copy the installation files to the StoreFront server and provide users with these local files instead.

For users who cannot install Citrix Receiver, you can enable Citrix Receiver for HTML5 on your Citrix Receiver for Web sites. Citrix Receiver for HTML5 enables users to access desktops and applications directly within HTML5-compatible web browsers without needing to install Citrix Receiver. Both internal network connections and connections through NetScaler Gateway are supported. However, for connections from the internal network, Citrix Receiver for HTML5 only enables access to resources provided by specific products. Additionally, specific versions of NetScaler Gateway are required to enable connections from outside the corporate network. For more information, see Infrastructure requirements.

For local users on the internal network, access through Citrix Receiver for HTML5 to resources provided by XenDesktop and XenApp is disabled by default. To enable local access to desktops and applications using Citrix Receiver for HTML5, you must enable the ICA WebSockets connections policy on your XenDesktop and XenApp servers. XenDesktop and XenApp use port 8008 for Citrix Receiver for HTML5 connections. Ensure your firewalls and other network devices permit access to this port. For more information, see WebSockets policy settings.

Citrix Receiver for HTML5 can only be used with Internet Explorer over HTTP connections. To use Citrix Receiver for HTML5 with Mozilla Firefox over HTTPS connections, users must type **about:config** in the Firefox address bar and set the **network.websocket.allowInsecureFromHTTPS** preference to **true**.

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a site. In the **Actions** pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Choose **Deploy Citrix Receiver** and specify the response of the Citrix Receiver for Web site if Citrix Receiver cannot be detected on a user's device.

- If you want the site to prompt the user to download and install the appropriate Citrix Receiver for their platform, select **Install locally**. Users must install Citrix Receiver to access desktops and applications through the site.
  - If you select **Allow users to download HDX engine (plug in)**, the Citrix Receiver for Web allows the user to download and install Citrix Receiver on the end user client if the Citrix Receiver is not available.
  - If you select **Upgrade plug-in at logon**, the Citrix Receiver for Web upgrades the Citrix Receiver client when the user logs on. To enable this feature, ensure the Citrix Receiver files are available on the StoreFront server.
  - Select a source from the drop-down menu.
- If you want the site to prompt the user to download and install Citrix Receiver but fall back to Citrix Receiver for HTML5

if Citrix Receiver cannot be installed, select **Use Receiver for HTML5 if local Receiver is unavailable**. Users without Citrix Receiver are prompted to download and install Citrix Receiver every time they log on to the site.

- If you want the site to enable access to resources through Citrix Receiver for HTML5 without prompting the user to download and install Citrix Receiver, select **Always use Receiver for HTML5**. With that option selected, users always access desktops and applications on the site through Citrix Receiver for HTML5, provided they use an HTML5-compatible browser. Users without an HTML5-compatible browser have to install the native Citrix Receiver.

By default, when a user accesses a Citrix Receiver for Web site from a computer running Windows or Mac OS X, the site attempts to determine whether Citrix Receiver is installed on the user's device. If Citrix Receiver cannot be detected, the user is prompted to download and install the appropriate Citrix Receiver for their platform from the Citrix website.

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a site. In the **Actions** pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Choose **Deploy Citrix Receiver** and **Source for Receivers**, and then browse to the installation files.

Before logging on to StoreFront, Citrix Receiver for Web prompts a user to install the latest Citrix Receiver if Citrix Receiver is not already installed on the user's computer (for Internet Explorer, Firefox, and Safari users) or the first time that the user visits the site (for Chrome users). Depending on the configuration, the prompt might also display if the user's installation of Citrix Receiver can be upgraded.

You can configure Citrix Receiver for Web to display the prompt after logging on to StoreFront.

1. On the **Windows Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select the site from the results pane.
3. In the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**.
4. Select **Advanced Settings** and check **Prompt to install Citrix Receiver after logon**.

Use the **Manage Receiver for Web Sites** in the **Actions** pane to delete a Citrix Receiver for Web site. When you remove a site, users can no longer use that webpage to access the store.

統合Citrix Receiverエクスペリエンスのサポート

May 22, 2017

StoreFrontは、**クラシック**と**統合**の両方のユーザーエクスペリエンスをサポートします。クラシックエクスペリエンスでは、配信は各Citrix Receiverのプラットフォームのユーザーエクスペリエンスに依存します。新しい統合エクスペリエンスは、集中管理されたHTML5ユーザーエクスペリエンスをすべてのWebおよびネイティブCitrix Receiverに配信します。これはカスタマイズとお勧めのアプリケーショングループの管理をサポートしています。

このバージョンのStoreFrontを使って作成されたストアは、デフォルトで統合エクスペリエンスを使用しますが、アップグレードされたものについては、デフォルトでクラシックエクスペリエンスとなります。統合エクスペリエンスをサポートするには、StoreFrontストアをReceiver for Webサイトに割り当てる必要があり、そのサイトが統合エクスペリエンスを使用するように構成する必要があります。

重要：制限付きゾーンにReceiver for Webサイトを追加した場合、統合エクスペリエンスはサポートされません。制限付きゾーンにReceiver for Webサイトを追加する必要がある場合、クラシックエクスペリエンスを使用するようにストアを設定します。

StoreFront管理コンソールを使って、次のCitrix Receiver for Web関連タスクを実行します。

- Citrix Receiver for Webサイトの作成。
- Citrix Receiver for Webサイトエクスペリエンスの変更。
- ストアに割り当てる統合Citrix Receiver for Webサイトの選択。
- Receiverの外観をカスタマイズします。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

> ## 注意
>
> XenApp 6.xを使用している場合、統合エクスペリエンスが有効な**[クライアントにストリーム配信する]**または**[ストリーム配信できない場合はサーバー上で実行する]**に設定したアプリケーションはサポートされません。

ストアを作成すると、Citrix Receiver for Webサイトが自動的に作成されます。また、次のことを実行して追加のReceiver for Webサイトを作成することもできます。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで［Receiver for Webサイトの管理］>［追加］の順にクリックしてウィザードの指示に従います。

Citrix Receiver for Webの Webサイトが**クラシック**または**統合**エクスペリエンスを配信するかどうかを選択できます。クラシックエクスペリエンスを有効にすると、詳細なカスタマイズとお勧めのアプリケーショングループの管理ができなくなります。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。

2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択し、真ん中のペインで変更するストアを選択して、［操作］ペインで **[Receiver for Webサイトの管理]**、次に **[構成]** の順にクリックします。
3. **[Receiverエクスペリエンス]** を選択し、**[クラシックエクスペリエンスの無効化]** または **[クラシックエクスペリエンスの有効化]** を選択します。

ストアに割り当てる統合Citrix Receiver for Webサイトの選択

StoreFrontを使って新しいストアが作成されると、統合モードのCitrix Receiver for Webサイトが自動的に作成され、ストアに割り当てられます。ただし、以前のバージョンのStoreFrontからアップグレードした場合は、デフォルトでクラシックエクスペリエンスに設定されます。

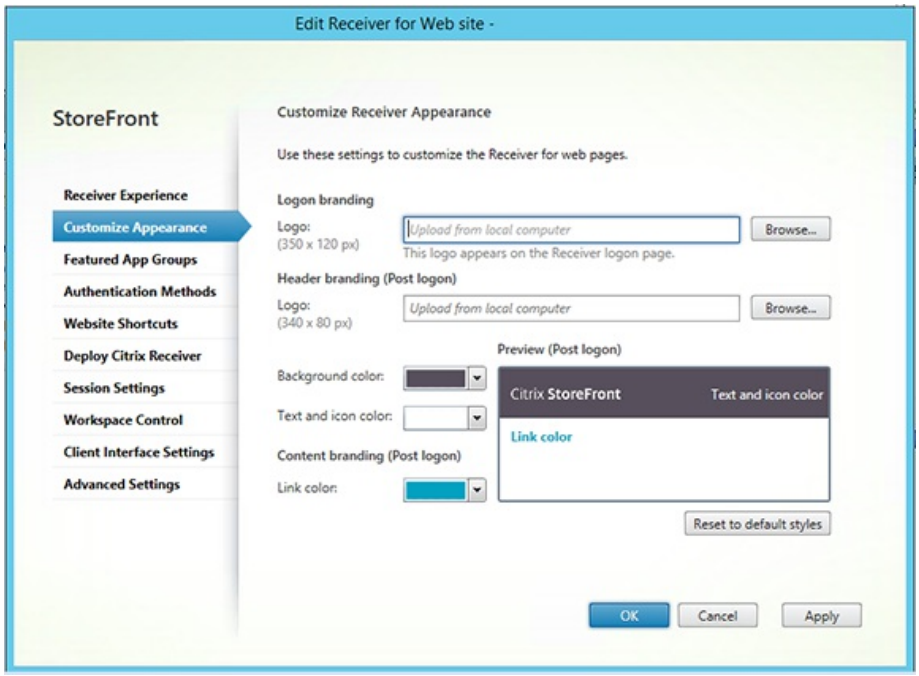
Citrix Receiver for Webサイトを選択してストアに統合エクスペリエンスを提供するには、クラシックエクスペリエンスを無効にして作成されたCitrix Receiver for Webサイトが1つ以上必要です。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、**[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択し、真ん中のペインでストアを選択して、**[操作]** ペインで **[統合エクスペリエンスの構成]** をクリックします。ストアのデフォルトとしては、（クラシックエクスペリエンスを無効にして）統合エクスペリエンスをサポートするWebサイトだけを使用できます。作成されたCitrix Receiver for WebのWebサイトがない場合は、新しいReceiver for WebのWebサイトの作成へのリンクを含むメッセージが表示されます。また、既存のReceiver for WebサイトをReceiver for WebのWebサイトに変更することもできます。「Citrix Receiverエクスペリエンス」を参照してください。
3. Citrix Receiver for Webサイトを作成したら、このストアの **[統合エクスペリエンスの構成]** を選択し、特定のWebサイトを選択します。

> **Important**
>
> Receiver for Webサイト上で統合エクスペリエンスをクラシックエクスペリエンスに変更する場合、ネイティブのCitrix Receiverクライアントに影響が及ぶ可能性があります。このReceiver fot Webサイト上でエクスペリエンスを統合エクスペリエンスに戻しても、ネイティブのCitrix Receiverクライアントのエクスペリエンスが統合エクスペリエンスに更新されることはありません。管理コンソールで［ストア］ノードの統合エクスペリエンスをリセットする必要があります。

Citrix Receiverの外観をカスタマイズするには、お使いのCitrix Receiver for WebのWebサイトでクラシックCitrix Receiverエクスペリエンスを無効にする必要があります。

1. Windowsの **[スタート]** 画面または［アプリ］画面で、**[Citrix StoreFront]** タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインで **[Receiver for Webサイトの管理]** > **[構成]** の順にクリックします。
3. **[Receiverエクスペリエンス]** > **[クラシックエクスペリエンスの無効化]** の順に選択します。
4. **[外観のカスタマイズ]** を選択し、項目を選択してログオン後のWebサイトの表示方法をカスタマイズします。



おすすめのアプリケーションの作成および管理

May 22, 2017

特定のカテゴリに関連するまたはそれと適合するエンドユーザーに対するお勧めのアプリケーショングループを作成できます。たとえば、営業部により使用されるアプリケーションを含む、営業部におすすめのアプリケーショングループを作成できます。アプリケーション名を使ったり、Studioコンソールで定義されたキーワードまたはあプリケーションカテゴリを使ったりして、StoreFront管理コンソールでおすすめのアプリケーションを定義できます。

［おすすめのアプリケーショングループ］タスクを使って、おすすめのアプリケーショングループを追加、編集、または削除します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

この機能は、クラシックエクスペリエンスを無効にした場合に限り使用できます。

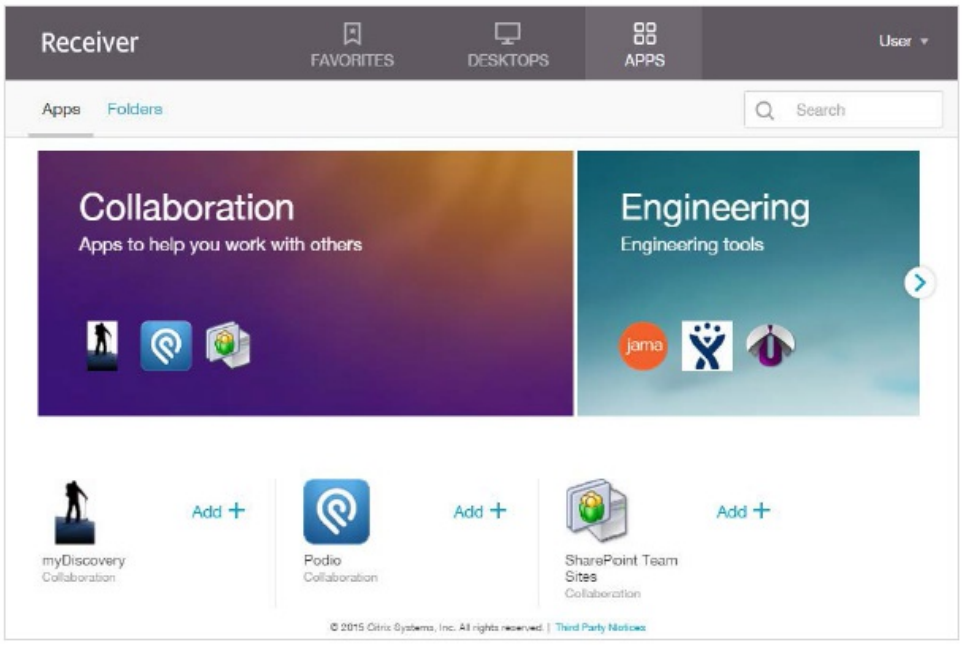
1. Windowsの **[スタート]** 画面または［アプリ］画面で、［Citrix**StoreFront**］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインで**[Receiver for Webサイトの管理]** > **[構成]** の順にクリックします。
3. **[おすすめのアプリケーショングループ]** を選択します。
4. **[おすすめのアプリケーショングループ]** ダイアログボックスで、**[作成]** をクリックして新しいお勧めのアプリケーショングループを定義します。
5. **[お勧めのアプリケーショングループの作成]** ダイアログボックスで、おすすめのアプリケーショングループ名、説明（任意）、背景、およびおすすめのアプリケーショングループを定義する方法を指定します。キーワード、アプリケーション名、またはアプリケーションカテゴリを選択し、**[OK]** をクリックします。

オプション	説明
キーワード	Studioでキーワードを定義します。
アプリケーションカテゴリ	Studioでアプリケーションカテゴリを定義します。
アプリケーション名	アプリケーション名を使っておすすめのアプリケーショングループを定義します。［お勧めのアプリケーショングループの作成］ダイアログボックスのここに含まれている名前と一致するすべてのアプリケーション名は、おすすめのアプリケーショングループに含まれます。 StoreFrontはアプリケーション名でワイルドカードをサポートしません。一致する内容では大文字と小文字は区別されませんが、全体が一致する必要があります。たとえば、「Excel」と入力すると、StoreFrontでは公開アプリケーション名のMicrosoft Excel 2013が一致となりますが、「Exc」と入力しても一致するものはありません。

たとえば、次のように指定します。

2つのおすすめアプリケーショングループを作成しました。

- コラボレーション - Studioの**Collaboration**カテゴリに含まれるアプリケーションとの一致を指定することによって作成しました。
- 開発 - アプリケーショングループに名前を付けて、アプリケーション名のコレクションを指定することによって作成しました。



ワークスペースコントロールの構成

May 22, 2017

ワークスペースコントロール機能を有効にすると、ユーザーがセッションの途中でデバイスを切り替えても、新しいデバイス上でそのアプリケーションでの作業を継続できます。これにより、たとえば病院で臨床医がほかのワークステーションに移動しても、移動先のデバイスでアプリケーションを起動し直す必要がなくなります。Citrix Receiver for Webサイトでは、ワークスペースコントロールがデフォルトで有効になります。ワークスペースコントロールを無効にしたり設定を変更したりするには、サイトの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、［Citrix StoreFront］タイルをクリックします。
2. 左ペインで **[ストア]** を選択し、［操作］ペインで **[Receiver for Webサイトの管理] >構成の順にクリックします。**
3. **[ワークスペースコントロール]** を選択します。
4. ワークスペースコントロールのデフォルト設定を構成します。以下の設定が含まれます。

    ワークスペースコントロールの有効化

    セッション再接続オプションの設定

    ログオフ操作の指定

Citrix Receiver for HTML5のブラウザータブ使用の構成

May 22, 2017

デフォルトでは、Citrix Receiver for HTML5は新しいブラウザータブでデスクトップやアプリケーションを起動します。ただし、ユーザーがCitrix Receiver for HTML5を使用してショートカットからリソースを起動した場合、既存のブラウザータブのCitrix Receiver for Webサイトが置き換わり、そこでデスクトップまたはアプリケーションが起動します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの **[スタート]** 画面または **[アプリ]** 画面で、［Citrix StoreFront］タイルをクリックします。
2. 左ペインで **[ストア]** を選択し、［操作］ペインで **[Receiver for Webサイトの管理]** >**構成**の順にクリックします。
3. **[Citrix Receiverの展開]** を選択します。
4. **[展開オプション]** ドロップダウンメニューから **[常にHTML 5 Receiverを使用する]** を選択し、アプリケーションを起動するタブに応じて、 **[Receiver for Webと同じタブでアプリケーションを起動]** をオンまたはオフにします。

通信のタイムアウト期間および再試行回数の構成

May 22, 2017

デフォルトでは、Citrix Receiver for Webサイトからそのストアへの要求は、3分でタイムアウトします。通信の試行が1回失敗すると、ストアが使用できないとみなされます。デフォルトの設定を変更するには、**[セッション設定]**タスクを使用します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの**[スタート]**画面または**[アプリ]**画面で、**[Citrix StoreFront]**タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで**[ストア]**ノードを選択し、真ん中のペインでストアを選択して、**[操作]**ペインで**[Receiver for Webサイトの管理]** > **[構成]の順にクリックします。**
3. **[セッション設定]**を選択し、変更を加えて**[OK/適用]**をクリックして、変更を保存します。

Configure user access

May 30, 2017

This article contains the following information:

> ## Important
>
> In multiple server deployments, use only one server at a time to change the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

Configure support for connections through XenApp Services URLs

Use the **Configure XenApp Services Support** task to configure access to your stores through XenApp Services URLs. Users of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with users who have older Citrix clients that cannot be upgraded, can access stores directly using the XenApp Services URL for the store. When you create a new store, the XenApp Services URL is enabled by default.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure XenApp Services Support**.
3. Select or clear the **Enable XenApp Services Support** check box to, respectively, enable or disable user access to the store through the displayed XenApp Services URL.
   The XenApp Services URL for a store has the form http[s]*://serveraddress/Citrix/storename/PNAgent/config.xml*, where *serveraddress* is the fully qualified domain name of the server or load balancing environment for your StoreFront deployment and *storename* is the name specified for the store when it was created.
4. If you enable XenApp Services Support, optionally specify a default store in your StoreFront deployment for users with the Citrix Online Plug-in.
   Specify a default store so that your users can configure the Citrix Online Plug-in with the server URL or load-balanced URL of the StoreFront deployment, rather than the XenApp Services URL for a particular store.

Disable or enable workspace control reconnect for all Citrix Receivers

Workspace control enables applications to follow users as they move between devices. This allows, for example, clinicians in

hospitals to move from workstation to workstation without having to restart their applications on each device.

StoreFront contains a configuration to disable workspace control reconnect in the Store Service for all Citrix Receivers. Manage this feature by using the StoreFront console or PowerShell.

Use the StoreFront management console

1. On the Windows **Start** screen or Apps screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Configure Store Settings**.
3. Select **Advanced Settings** and check or uncheck **Allow session reconnect**.

Use PowerShell

Make sure that you close the Administration Console. Run the following code snippet to import the StoreFront PowerShell modules:

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

Then the PowerShell command **Set-DSAllowSessionReconnect** turns Workspace control reconnect on or off.

Syntax

```
Set-DSAllowSessionReconnect [[-SiteId] <Int64>] [[-VirtualPath] <String> ] `
[[-IsAllowed] <Boolean>]
```

For example, to turn off workspace control reconnect for a store in /Citrix/Store, the following command configures the store:

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

Configure user subscriptions

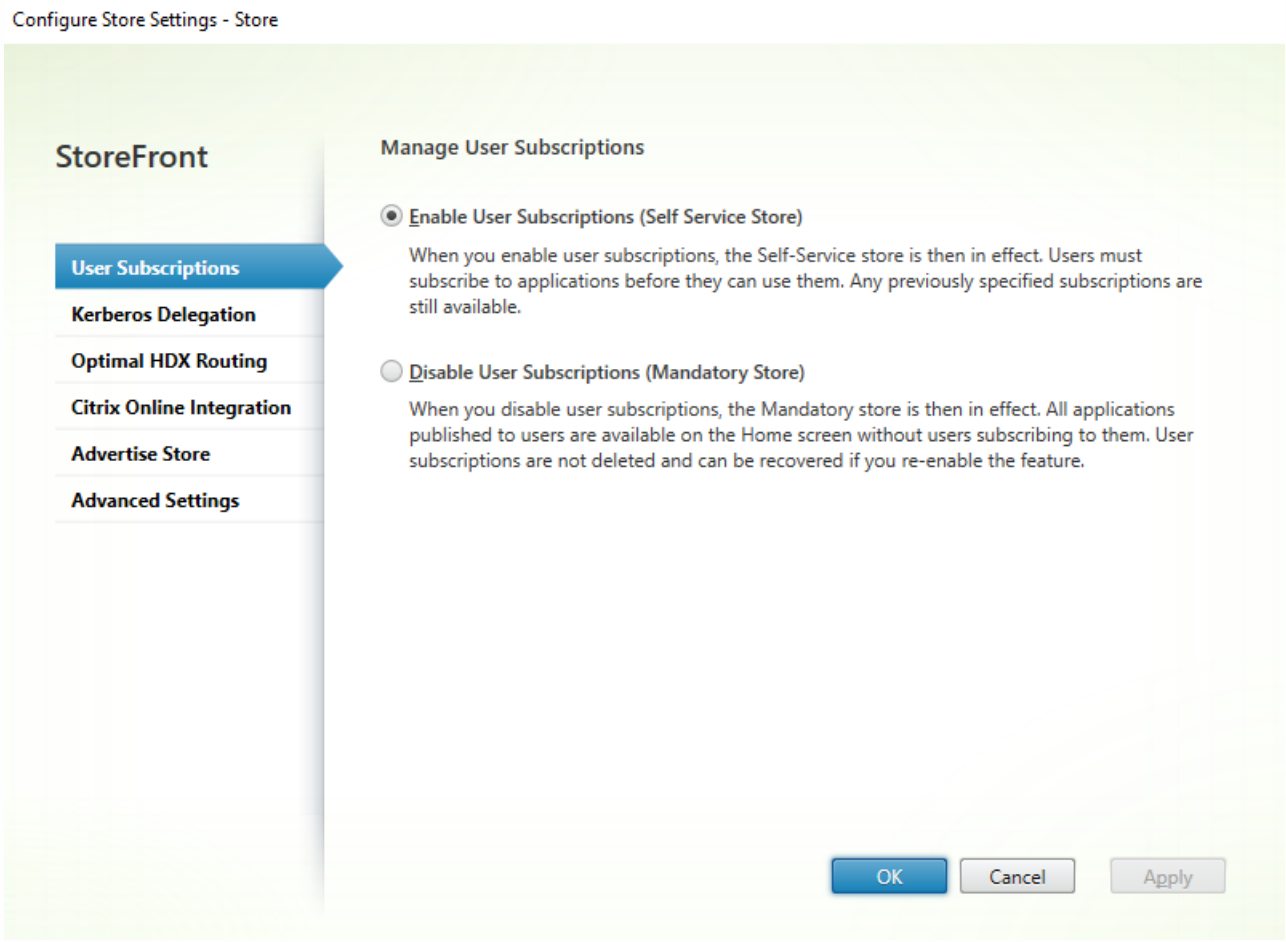
Use the User Subscriptions task to do select one of the following options:

- Require users to subscribe to applications before using them (Self Service Store).
- Enable users to receive all applications when they connect to the store (Mandatory Store).

Disabling user subscriptions for a store within StoreFront also prevents the display of the Favorites tab to users in Citrix Receiver. Disabling subscriptions does not delete the Store subscription data. Re-enabling subscriptions for the store will allow the user to see their subscribed apps in Favorites whenever they next log on.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings** > **User Subscriptions** to toggle the user subscriptions feature off or on.
3. Choose **Enable user subscriptions (Self Service Store)** to make users subscribe to the applications to use them. Any previously specified subscriptions are still available.
4. Choose **Disable user subscriptions (Mandatory Store)** to make all applications published to the users available on the

Home screen without users subscribing to them. Their subscriptions are not deleted and they can recover them if you re-enable the feature.



In StoreFront 3.5 or later, you can use the following PowerShell script to configure user subscriptions for a store:

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

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

For more information on Get-STFStoreService, see https://citrix.github.io/storefront-sdk/Citrix.StoreFront.Stores/Get-STFStoreService/

Manage subscription data for a store

Manage subscription data for a store using PowerShell cmdlets.

> **注意**
>
> Use either the StoreFront management console or PowerShell to manage StoreFront. Do not use both methods at the same time. Always close the StoreFront management console before using PowerShell to change your StoreFront configuration. Citrix also recommends that you take a backup of your existing subscription data before making changes so that rollback to a previous state is possible.

Purge subscription data

A folder and datastore containing subscription data exists for each store in your deployment.

1. Stop the Citrix Subscriptions Store service on the StoreFront server. If the Citrix Subscriptions Store service is running, it is not possible to delete subscription data for any of your stores.
2. Locate the subscription store folder on the StoreFront server: C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
3. Delete the contents of the subscription store folder, but do not delete the folder itself.
4. Restart the Citrix Subscriptions Store service on the StoreFront server.

In StoreFront 3.5 or later, you can use the following PowerShell script to purge subscription data for a store. Run this PowerShell function as an administrator with rights to stop or start services and delete files. This PowerShell function achieves the same result as the manual steps described above.

To run the cmdlets successfully, the Citrix Subscriptions Store service must be running on the server.

Code コピー

```
function Remove-SubscriptionData

{

    [CmdletBinding()]

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

    $SubsService = "Citrix Subscriptions Store"

    # Path to Subscription Data in StoreFront version 2.6 or higher

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

    Stop-Service -displayname $SubsService

    Remove-Item $SubsPath -Force -Verbose

    Start-Service -displayname $SubsService

    Get-Service -displayname $SubsService

}



Remove-SubscriptionData -Store "YourStore"
```

Export subscription data

You can obtain a backup of the Store subscription data in the form of a tab separated .txt file using the following PowerShell cmdlet.

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

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

If you are managing a multiple-server deployment, you can run this PowerShell cmdlet on any server within the StoreFront server group. Each server in the server group maintains an identical synced copy of the subscription data from its peers. If you believe you are experiencing issues with subscription synchronization between the Storefront servers, then export the data from all servers in the group and compare them to see differences.

Restore subscription data

Use Restore-STFStoreSubscriptions to overwrite your existing subscription data. You can restore a Store's subscription data using the tab separated .txt file backup you created earlier using Export-STFStoreSubscriptions.

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

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

For more information on Restore-STFStoreSubscriptions, see https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Restore-STFStoreSubscriptions/#restore-stfstoresubscriptions

Restoring Data on a Single StoreFront Server

In a single server deployment, there is no need to shut down the Subscriptions Store service. There is also no need to purge the existing subscription data before restoring the subscription data.

Restoring Data on a StoreFront Server Group

To restore subscription data to a server group, the following steps are required.

Example Server Group Deployment containing three StoreFront servers.

StoreFrontA

StoreFrontB

StoreFrontC

1. Back up of the existing subscription data from any of the three servers.
2. Stop the Subscriptions Store service on servers StoreFrontB and C. This action prevents the servers from sending or receiving subscription data during the update of StoreFrontA.
3. Purge the subscription data from servers StoreFrontB and C. This action prevents mismatch of the restored subscription data.
4. Restore the data on StoreFrontA using the Restore-STFStoreSubscriptions cmdlet. It is not necessary to stop the Subscriptions Store service, or to purge the subscription data on StoreFrontA (it is overwritten during the restore operation).
5. Restart the Subscriptions Store service on servers StoreFrontB and StoreFrontC. The servers can then receive a copy of the data from StoreFrontA.
6. Wait for synchronization to occur between all servers. The time required depends on the number of records that exist on StoreFrontA. If all servers are on a local network connection, synchronization normally occurs quickly. Synchronization of subscriptions across a WAN connection may take longer.
7. Export the data from StoreFrontB and C to confirm that the synchronization has completed, or view the Store Subscription counters.

Import subscription data

Use Import-STFStoreSubscriptions when there is no subscription data for the Store. This cmdlet also allows subscription data to be transferred from one Store to another or if subscription data is imported to newly provisioned StoreFront servers.

Code コピー

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


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

For more information on Import-STFStoreSubscriptions, see https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Import-STFStoreSubscriptions/#import-stfstoresubscriptions

Subscription data file details

The subscription data file is a text file containing one line per user subscription. Each line is a tab-separated sequence of values:

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

The values are defined as follows:

- <*user-identifier*> - Required. A sequence of characters identifying the user. This identifier is the user's Windows Security Identifier.
- <*resource-id*> - Required. A sequence of characters identifying the subscribed resource.
- <*subscription-id*> - Required. A sequence of characters uniquely identifying the subscription. This value is not used (although, a value must be present in the data file).
- <*subscription-status*> - Required. The status of the subscription: subscribed or unsubscribed.
- <*property-name*> and <*property-value*> -Optional. A sequence of zero or more pairs of <property-name> and <property-value> values. These represent properties associated with the subscription by a StoreFront client (typically a Citrix Receiver). A property with multiple values that is represented by multiple name/value pairs that have the same name (for example, "... MyProp A MyProp B ..." represents the property MyProp with values A, B).

Example:

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

Size of subscription data on the StoreFront server disk

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

Size of import and export .txt files

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

Store Subscription Counters

You can use Microsoft Windows Performance Monitor counters (Start > Run > perfmon) to show, for example, the total numbers of subscription records on the server or number of records synchronized between StoreFront server groups.

View the Subscription Counters using PowerShell

Code コピー

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

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

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

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

Set up highly available multi-site stores

May 22, 2017

In this article:

For stores that aggregate resources from multiple deployments, particularly geographically dispersed deployments, you can configure load balancing and failover between deployments, mapping of users to deployments, and specific disaster recovery deployments to provide highly available resources. Where you have configured separate NetScaler Gateway appliances for your deployments, you can define the optimal appliance for users to access each of the deployments.

Since StoreFront 3.5, the StoreFront management console has supported common multi-site scenarios. Citrix recommends you use the management console when it meets your requirements.

Configure user mapping and aggregation

The StoreFront management console enables you to:

- **Map users to deployments:** Based on Active Directory group membership, you can limit which users have access to particular deployments.
- **Aggregate deployments:** You can specify which deployments have resources that you want to aggregate. Matching resources from aggregated deployments are presented to the user as a single highly-available resource.
- **Associate a zone with a deployment:** When accessed with NetScaler Gateway in a global load-balancing configuration, StoreFront prioritizes deployments from zones matching the gateway zone when launching resources.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. Ensure that you have configured the store with details of all the XenDesktop and XenApp deployments that you want to use in your configuration. For more information about adding deployments to stores, see Manage the resources made available in stores.
2. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
3. Select the **Stores** node in the left pane of the Citrix StoreFront management console and click **Manage Delivery Controllers** in the **Actions** pane.
4. If two or more controllers are defined, click **User Mapping and Multi-Site Aggregation Configuration > Configure**.

5. Click **Map users to controllers** and make selections on the screens to specify which Delivery Controllers are available to which users.
6. Click **Aggregate resources**, choose controllers, and click **Aggregate** to specify whether or not Delivery Controllers are aggregated. If you enable aggregation of Delivery Controllers, applications and desktops from those Delivery Controllers with the same display name and path are presented as a single application/desktop in Citrix Receiver.
7. Choose one, or both, of the **Aggregated Controller Settings** check boxes and click **OK**.

   Controllers publish identical resources - When checked, StoreFront enumerates resources from only one of the controllers in the aggregated set. When unchecked, StoreFront enumerates resources from all controllers in the aggregated set (to accumulate the user's entire set of available resources). Checking this option gives a performance improvement when enumerating resources, but we do not recommend it unless you are certain that the list of resources is identical across all aggregated deployments.

   Load balance resources across controllers - When checked, launches are distributed evenly among the available controllers. When unchecked, launches are directed to the first controller specified in the user mapping dialog screen, failing over to subsequent controllers if the launch fails.

Advanced configurations

Although you can configure many common multi-site and high availability operations with the StoreFront management console, you can still configure StoreFront using the configuration files in the same manner as earlier StoreFront versions.

Extra functionality available using PowerShell or by editing the StoreFront configuration files:

- The ability to specify multiple groupings of deployments for aggregation.
  - The management console allows only a single grouping of deployments, which is sufficient for most cases.
  - For stores with many deployments with disjointed sets of resources, multiple groupings might give performance improvements.
- The ability to specify complex preference orders for aggregated deployments. The management console allows aggregated deployments to be load balanced or to be used as a single failover list.
- The ability to define disaster recovery deployments (deployments accessed only when all other deployments are unavailable).

Warning: After configuring advanced multi-site options by manually editing the configuration file, some tasks become unavailable in the Citrix StoreFront management console to prevent misconfiguration.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. Ensure that you have configured the store with details of all the XenDesktop and XenApp deployments that you want to use in your configuration, including disaster recovery deployments. For more information about adding deployments to stores, see Manage the resources made available in stores.
2. Use a text editor to open the web.config file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix\storename\ directory, where storename is the name specified for the store when it was created.
3. Locate the following section in the file.
   <resourcesWingConfigurations>
   <resourcesWingConfiguration name="Default" wingName="Default" />


```
</resourcesWingConfigurations>
```

4. Specify your configuration as shown below.

```
<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>
```

Use the following elements to define your configuration.

- **userFarmMapping**
  Specifies groups of deployments and defines the load balancing and failover behavior between those deployments. Identifies deployments to be used for disaster recovery. Controls user access to resources by mapping Microsoft Active Directory user groups to the specified groups of deployments.
- **groups**
  Specifies the names and security identifiers (SIDs) of Active Directory user groups to which the associated mapping

applies. User group names must be entered in the format *domain**usergroup*. Where more than one group is listed, the mapping is only applied to users who are members of all the specified groups. To enable access for all Active Directory user accounts, set the group name & sid to **everyone**.

- **equivalentFarmSet**
  Specifies a group of equivalent deployments providing resources to be aggregated for load balancing or failover, plus an optional associated group of disaster recovery deployments.

  The **loadBalanceMod**e attribute determines the allocation of users to deployments. Set the value of the **loadBalanceMode** attribute to **LoadBalanced** to randomly assign users to deployments in the equivalent deployment set, evenly distributing users across all the available deployments. When the value of the **loadBalanceMode** attribute is set to **Failover**, users are connected to the first available deployment in the order in which they are listed in the configuration, minimizing the number of deployments in use at any given time. Specify names for aggregation groups to identify equivalent deployment sets providing resources to be aggregated. Resources provided by equivalent deployment sets belonging to the same aggregation group are aggregated. To specify that the deployments defined in a particular equivalent deployment set should not be aggregated with others, set the aggregation group name to the empty string **""**.

  The **identical** attribute accepts the values **true** and **false**, and specifies whether all deployments within an equivalent deployment set provide exactly the same set of resources. When the deployments are identical, StoreFront enumerates the user's resources from just one primary deployment in the set. When the deployments provide overlapping but not identical resources, StoreFront enumerates from each deployment to obtain the full set of resources available to a user. Load balancing (at launch time) can take place whether or not the deployments are identical. The default value for the **identical** attribute is false, although it is set to **true** when StoreFront is upgraded to avoid altering the pre-existing behavior following an upgrade.

- **primaryFarmRefs**
  Specifies a set of equivalent XenDesktop or XenApp sites where some or all of the resources match. Enter the names of deployments that you have already added to the store. The names of the deployments you specify must match exactly the names you entered when you added the deployments to the store.
- **optimalGatewayForFarms**
  Specifies groups of deployments and defines the optimal NetScaler Gateway appliances for users to access resources provided by these deployments. Typically, the optimal appliance for a deployment is colocated in the same geographical location as that deployment. You only need to define optimal NetScaler Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal appliance.

Configure subscription synchronization

To configure periodic pull synchronization of users' application subscriptions from stores in different StoreFront deployments, you execute Windows PowerShell commands.

Note: The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.
Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server groups so that the other servers in the deployment are updated.
When establishing your subscription synchronization, note that the configured Delivery Controllers must be named

identically between the synchronized Stores and that the Delivery Controller names are case sensitive. Failing to duplicate the Delivery Controller names exactly may lead to users having different subscriptions across the synchronized Stores.

1. Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, type the following commands to import the StoreFront modules.
   Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1"
   Import-Module "installationlocation\Management\Cmdlets\
   SubscriptionSyncModule.psm1"
   Where installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\.

2. To specify the remote StoreFront deployment containing the store to be synchronized, type the following command.
   Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname
   -clusterAddress deploymentaddress
   Where deploymentname is a name that helps you identify the remote deployment and deploymentaddress is the externally accessible address of the StoreFront server or load-balanced server group for the remote deployment.

3. To specify the remote store with which to synchronize users' application subscriptions, type the following command.
   Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname
   -storeName storename
   Where deploymentname is the name that you defined for the remote deployment in the previous step and storename is the name specified for both the local and remote stores when they were created. To synchronize application subscriptions between the stores, both stores must have the same name in their respective StoreFront deployments.

4. To configure synchronization to occur at a particular time every day, type the following command.
   Add-DSSubscriptionsSyncSchedule -scheduleName
   synchronizationname -startTime hh:mm
   Where synchronizationname is a name that helps you identify the schedule you are creating. Use the -startTime setting to specify a time of day at which you want to synchronize subscriptions between the stores. Configure further schedules to specify additional synchronization times throughout the day.

5. Alternatively, to configure regular synchronization at a specific interval, type the following command.
   Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName
   synchronizationname -startTime hh:mm:ss -repeatMinutes interval
   Where synchronizationname is a name that helps you identify the schedule you are creating. Use the -startTime setting to specify the a time of day at which you want to start the reoccurring schedule. For interval, specify the time in minutes between each synchronization.

6. Add the Microsoft Active Directory domain machine accounts for each StoreFront server in the remote deployment to the local Windows user group CitrixSubscriptionSyncUsers on the current server.
   This will allow the servers in the remote deployment to access the subscription store service on the local deployment once you have configured a synchronization schedule on the remote deployment. The CitrixSubscriptionSyncUsers group is automatically created when you import the subscription synchronization module in Step 1. For more information about modifying local user groups, see http://technet.microsoft.com/en-us/library/cc772524.aspx.

7. If your local StoreFront deployment consists of multiple servers, use the Citrix StoreFront management console to propagate the configuration changes to the other servers in the group.
   For more information about propagating changes in a multiple server StoreFront deployment, see Configure server groups.

8. Repeat Steps 1 to 7 on the remote StoreFront deployment to configure a complementary subscription synchronization schedule from the remote deployment to the local deployment.
   When configuring the synchronization schedules for your StoreFront deployments, ensure that the schedules do not lead to a situation where the deployments are attempting to synchronize simultaneously.

9. To start synchronizing users' application subscriptions between the stores, restart the subscription store service on both the local and remote deployments. At a Windows PowerShell command prompt on a server in each deployment, type the following command.
   Restart-DSSubscriptionsStoreSubscriptionService
10. To remove an existing subscription synchronization schedule, type the following command. Then, propagate the configuration change to the other StoreFront servers in the deployment and restart the subscription store service.
    Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
    Where synchronizationname is the name that you specified for the schedule when you created it.

11. To list the subscription synchronization schedules currently configured for your StoreFront deployment, type the following command.
    Get-DSSubscriptionsSyncScheduleSummary

Configure optimal HDX routing for a store

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

The difference between a farm and a zone when defining optimal gateway mappings for a store

In StoreFront versions released before 3.5, you could map an optimal gateway only to a farm or farms. The concept of zones enables you to divide a XenApp 7.8 or XenDesktop 7.8 deployment into zones based on the data center or geographic location where the XenApp or XenDesktop controllers and published resources reside. Define zones in XenApp or XenDesktop 7.8 Studio. StoreFront now interoperates with XenApp 7.8 and XenDesktop 7.8 and any zones defined in StoreFront must exactly match the zone names defined in XenApp and XenDesktop.

This version of StoreFront also allows you to create an optimal gateway mapping for all of the delivery controllers located in the defined zone. Mapping a zone to an optimal gateway is almost identical to creating mappings using farms, with which you might already be familiar. The only difference is that zones typically represent much larger containers with many more delivery controllers. You do not need to add every delivery controller to an optimal gateway mapping. To place the controllers into the desired zone, you need only tag each delivery controller with a zone name that matches a zone already defined in XenApp or XenDesktop. You can map an optimal gateway to more than one zone, but typically you should use a single zone. A zone usually represents a data center in a geographic location. It is expected that each zone has at least one optimal NetScaler Gateway that is used for HDX connections to resources within that zone.

For more information about zones, see Zones.

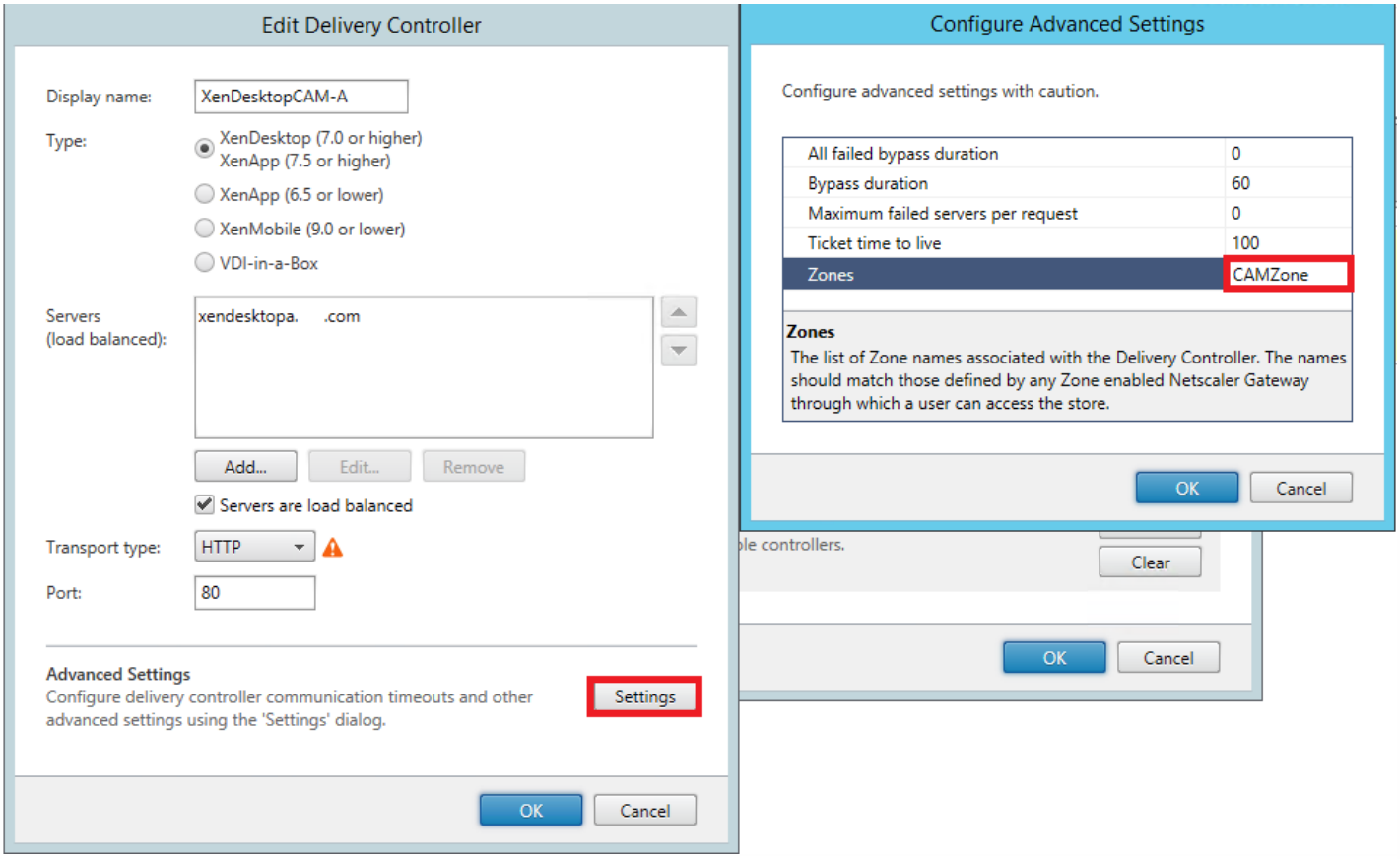
Place a delivery controller into a zone

Set the zone attribute on every delivery controller you wish to place within a Zone.

1. On the Windows **Start** screen or Apps screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and click **Manage Delivery**

Controllers in the **Actions** pane.

3. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
4. On the **Zones** row, click in the second column.
5. Click **Add** on the **Delivery Controller Zone Names** screen and then add a zone name.



Configure optimal NetScaler Gateway routing to optimize the handling of ICA connection routing from the HDX engine to published resources such as XenDesktop VDAs or XenApp or XenDesktop published applications using StoreFront. Typically, the optimal gateway for a site is collocated in the same geographical location.

You need only define optimal NetScaler Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal gateway. If launches should be directed back through the gateway making the launch request, StoreFront does this automatically.

Example scenario using farms

1 x UK Gateway -> 1 x UK StoreFront	-> UK Apps and Desktops local
	-> US Apps and Desktops used only for UK failover
1 x US Gateway -> 1 x US StoreFront	-> US Apps and Desktops local
	-> UK Apps and Desktops used only for US failover

A UK gateway provides remote access to UK hosted resources such as apps and desktops using a UK StoreFront.

The UK storefront has both a UK based and US based NetScaler Gateway defined and UK and US farms in its delivery controller list. UK users access remote resources through their geographically collocated gateway, StoreFront, and farms. If their UK resources become unavailable, they can connect to US resources as a temporary failover alternative.

Without optimal gateway routing all ICA launches would pass through the UK gateway that made the launch request regardless of where the resources are geographically located. By default, gateways used to make launch requests are identified dynamically by StoreFront when the request is made. Optimal gateway routing overrides this and forces US connections through the gateway closest to the US farms that provides apps and desktops.

Note: You can map only a single optimal gateway per site for each StoreFront store.

Example scenario using zones

1 x CAMZone -> 2 x UK StoreFronts	-> Cambridge, UK: Apps and Desktops -> Fort Lauderdale, Eastern US: Apps and Desktops -> Bangalore, India: Apps and Desktops
1 x FTLZone -> 2 x US StoreFronts	-> Fort Lauderdale, Eastern US: Apps and Desktops -> Cambridge, UK: Apps and Desktops -> Bangalore, India: Apps and Desktops
1 x BGLZone -> 2 x IN StoreFronts	-> Bangalore, India: Apps and Desktops -> Cambridge, UK: Apps and Desktops -> Fort Lauderdale, Eastern US: Apps and Desktops

Figure 1. Suboptimal gateway routing

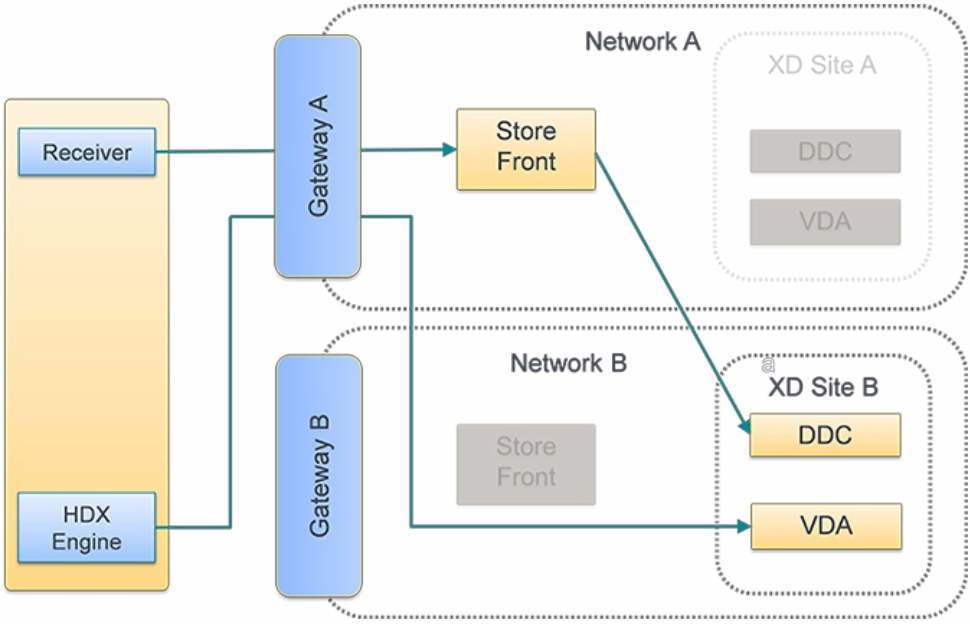
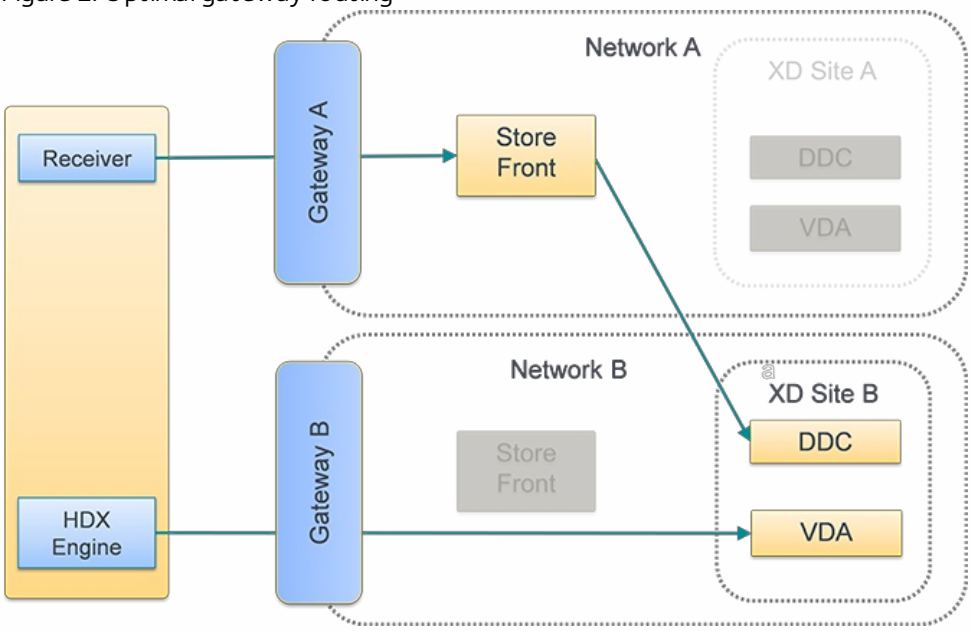


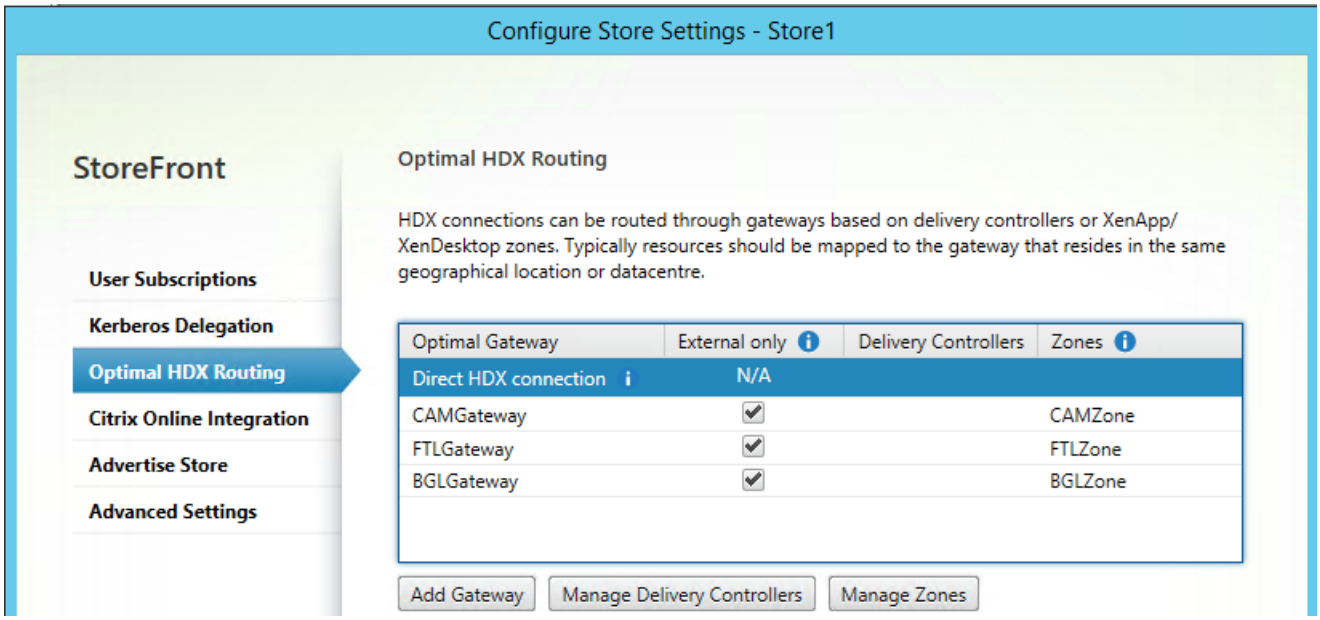
Figure 2. Optimal gateway routing



Use the Citrix StoreFront management console

After you configure separate NetScaler Gateway appliances for your deployments, you can define the optimal appliance for users to access each of the deployments.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings**.
3. On the **Settings** > **Optimal HDX Routing** page, select a gateway.
4. If you select the **External Only** check box, it is equivalent to **-enabledOnDirectAccess = false** and Direct HDX Connection is equivalent to using **Set-DSFarmsWithNullOptimalGateway** for farms or zones.



Add a new gateway

One of the options in the previous procedure is to **Add gateway**. After you choose **Add gateway**, the Add NetScaler Gateway screen displays.

1. On the **General Settings** screen, complete the Display name, NetScaler Gateway URL, and Usage or Role settings to configure access to stores through NetScaler Gateway for users connecting from public networks. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores.
2. On the **Secure Ticket Authority (STA)** screen, complete the options displayed. STA is hosted on XenDesktop and XenApp servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop and XenApp resources.
3. On the **Authentication Settings** screen, enter the settings that specify how the remote user provides authentication credentials.

Use PowerShell to configure optimal NetScaler Gateway routing for a store

PowerShell API parameters

Parameter	Description
-SiteId (Int)	Site ID within IIS. This is typically 1 for the site in IIS where StoreFront is installed by default.
-ResourcesVirtualPath (String)	Path to the store that is to be configured to have a farm to optimal gateway mapping. Example: "/Citrix/Store"
-GatewayName (String)	Name given to identify the Netscaler Gateway within StoreFront. Example 1: ExternalGateway Example 2: InternalGateway

-Hostnames (String Array)	Specifies the fully qualified domain name (FQDN) and port of the optimal NetScaler Gateway appliance. Example1 for standard vServer port 443: gateway.example.com Example2 for nonstandard vServer port 500: gateway.example.com:500
-Farms (String Array)	Specifies a set of (typically collocated) XenDesktop, XenApp, and App Controller deployments that share a common optimal NetScaler Gateway appliance. A farm can contain just a single delivery controller or multiple delivery controller that provides published resources. You can configure a XenDesktop site in StoreFront under delivery controllers as "XenDesktop". This represents a single farm. This could contain multiple delivery controllers in its failover list: Example: "XenDesktop" XenDesktop-A.example.com XenDesktop-B.example.com XenDesktop-C.example.com
-Zones (String Array)	Specifies a data center or data centers containing many delivery controllers. This requires you tag delivery controller objects in StoreFront with the appropriate zone to which you want to allocate them.
-staUrls (String Array)	Specifies the URLs for XenDesktop or XenApp servers running the Secure Ticket Authority (STA). If using multiple farms, list the STA servers on each using a comma separated list: Example: "http://xenapp-a.example.com/scripts/ctxsta.dll","http://xendesktop-a.example.com/scripts/ctxsta.dll"
-StasUseLoadBalancing (Boolean)	Set to true: randomly obtains session tickets from all STAs, evenly distributing requests across all the STAs. Set to false: users are connected to the first available STA in the order in which they are listed in the configuration, minimizing the number of STAs in use at any given time.
-StasBypassDuration	Set the time period, in hours, minutes, and seconds, for which an STA is considered unavailable after a failed request. Example: 02:00:00
-EnableSessionReliability (Boolean)	Set to true: keeps disconnected sessions open while Receiver attempts to reconnect automatically. If you configured multiple STAs and want to ensure that session reliability is always available, set the value of the useTwoTickets attribute to true to obtain session tickets from two different STAs in case one STA becomes unavailable during the session.
-UseTwoTickets (Boolean)	Set to true: obtains session tickets from two different STAs in case one STA becomes unavailable during the session. Set to false: uses only a single STA server.
-EnabledOnDirectAccess (Boolean)	Set to true: ensures that when local users on the internal network log on to StoreFront directly, connections to their resources are still routed through the optimal appliance defined for the farm. Set to false: connections to resources are not routed through the optimal appliance for the farm unless users access StoreFront through a NetScaler Gateway.

Note: When PowerShell scripts span multiple lines such as shown below, each line must end with the backtick character.

Citrix recommends copying any code examples into the Windows PowerShell Integrated Scripting Environment (ISE) to validate the Powershell code using the format checker before you run it.

Configure an optimal gateway for a farm

Example:

Create or overwrite Optimal Gateway For Farms mappings for the 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
```

Configure an optimal gateway for a zone

Example:

Create or overwrite Optimal Gateway For Farms mappings for the 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
```

Example:

This script returns all Optimal Gateway For Farms mappings for the store called Internal.

Get-DSOptimalGatewayForFarms -SiteId 1 –ResourcesVirtualPath "/Citrix/Internal"

Example:

Remove all optimal gateway for farms mappings for store called Internal.

Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"

Configure direct HDX connections for farms

Example:

This script prevents all ICA launches from passing through a gateway for the list of specified farms for the store calledInternal.

Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/Store -Farms "Farm1","Farm2"

Example:

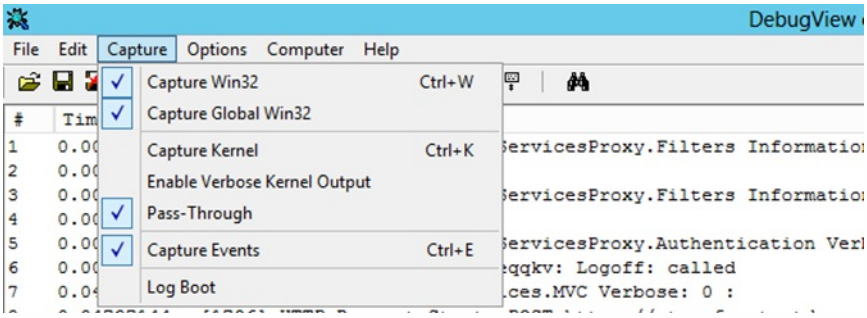
This script returns all farms that are configured to prevent ICA launches from passing through a gateway for a store called Internal.

Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"

Determine if your Optimal Gateway For Farms mappings are being used by StoreFront

1. Enable StoreFront tracing on all server group nodes using PowerShell by running:
   & "$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. Open the Debug View tool on the desktop of a StoreFront server. If you are using a storefront server group, you might have to do this on all nodes to ensure you obtain traces from the node that receives the launch request.
3. Enable Capture Global Win32 events.



4. Save the trace output as a .log file and open the file with Notepad. Search for the log entries shown in the example scenarios below.
5. Turn tracing off afterwards, as it consumes a lot of disk space on your StoreFront servers.
   Set-DSTraceLevel -All -TraceLevel Off

Tested optimal gateway scenarios

- External client logs on **Gateway1**. Launch is directed through the designated optimal gateway **Gateway2** for the farm **Farm2**.
  Set-DSOptimalGatewayForFarms -onDirectAccess=false

  Farm2 is configured to use the optimal gateway Gateway2.

  Farm2 has optimal gateway on direct access disabled.

  The optimal gateway Gateway2 will be used for the launch.

- Internal client logs on using StoreFront. Launch is directed through the designated optimal gatewayGateway1 for the farm Farm1.
  S**et-DSOptimalGatewayForFarms -onDirectAccess=true**

  No dynamically identified gateway in request. StoreFront was contacted directly.

  Farm1 is configured to use the optimal gateway Gateway1.

  Farm1 has optimal gateway on direct access enabled.

  The optimal gateway Gateway1 will be used for the launch.

- Internal client logs on using Gateway1. Launches of resources on Farm1 are prevented from passing through any gateway and StoreFront is contacted directly.
  Set-DSFarmsWithNullOptimalGateway

  Dynamically identified gateway in request: Gateway1

  Farm1 is configured to not use a gateway. No gateway will be used for launch.

NetScaler GatewayおよびNetScalerの統合

May 22, 2017

NetScaler GatewayをStoreFrontと一緒に使って、企業ネットワークとNetScalerの外側にいるユーザーにセキュアなリモートアクセスを提供し、負荷分散を実行します。

ゲートウェイとサーバー証明書の使用方法の計画

StoreFrontをNetScaler GatewayおよびNetScalerと統合するには、ゲートウェイとサーバー証明書の使用方法について計画を立てる必要があります。展開環境内のどのCitrixコンポーネントでサーバー証明書を要求するかを検討してください。

- インターネットに接続するサーバーおよびゲートウェイの証明書を外部の証明機関から取得する計画を立ててください。クライアントデバイスでは、内部証明機関により署名された証明書は自動で信頼されない場合があります。
- 外部および内部の両方のサーバー名を用意してください。多くの組織では、example.com（外部用）とexample.net（内部用）というように内部用と外部用の名前空間が分けられています。サブジェクトの別名（SAN）拡張機能を使用すると、これら両種の名前を1つの証明書に含めることができます。これは推奨される構成ではありません。公的証明機関から証明書が発行されるのは、最上位ドメイン（TLD：top-level domain）がIANAに登録されている場合のみです。この場合でも、一般的に使用される内部サーバー名の一部（example.localなど）は使用できないため、外部名と内部名で別々の証明書が必要になることがあります。
- 可能であれば、外部サーバーと内部サーバーには別の証明書を使用してください。ゲートウェイでは、各インターフェイスに異なる証明書をバインドすることで複数の証明書を使用できる場合があります。
- インターネットに接続するサーバーと接続しないサーバー間で証明書を共有しないでください。これらの証明書は、有効期間や失効ポリシーなどが内部証明機関から発行された証明書とは異なる可能性があります。
- 「ワイルドカード」証明書を共有するのは、同等のサービス間のみにしてください。異なる種類のサーバー間（StoreFrontサーバーとその他の種類のサーバーなど）で証明書を共有しないでください。異なる管理下にあるサーバー間やセキュリティポリシーが違うサーバー間で証明書を共有しないでください。 同等のサービスを提供するサーバーの典型的な例は以下のとおりです。
  - StoreFrontサーバーのグループとこれらのサーバー間で負荷分散を実行するサーバー。
  - GSLB内のインターネットに接続するゲートウェイのグループ。
  - 同等のリソースを提供するXenAppおよびXenDesktop 7.x Controllerのグループ。
- ハードウェアセキュリティで保護された秘密キーストレージを用意してください。一部のNetScalerモデルを含むゲートウェイとサーバーでは、ハードウェアセキュリティモジュール（HSM：Hardware Security Module）またはトラステッドプラットフォームモジュール（TPM：Trusted Platform Module）内に秘密キーを格納して保護することができます。セキュリティ上の理由から、こうした構成は、一般に証明書および秘密キーの共有をサポートするようには設定されていません。各コンポーネントのドキュメントを参照してください。 NetScaler Gatewayを使用してGSLBを実装する場合、使用するFQDNがすべて含まれる同一の証明書をGSLB内の各ゲートウェイに設定する必要のある場合があります。

Citrix展開環境のセキュリティ保護について詳しくは、「End-To-End Encryption with XenApp and XenDesktop」ホワイトペーパーおよびXenAppとXenDesktopの「セキュリティ保護」セクションを参照してください。

NetScaler Gateway接続の追加

May 22, 2017

ユーザーがストアにアクセスするときに経由するNetScaler Gateway展開環境を追加するには、[NetScaler Gatewayアプライアンスの追加]タスクを使用します。NetScaler Gatewayを経由するストアへのリモートアクセスを構成するには、その前に認証方法としてNetScaler Gatewayからのパススルーを有効にする必要があります。StoreFrontでのWebFront Gatewayの構成について詳しくは、「Using WebFront to Integrate with StoreFront」を参照してください。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［操作］ペインの［NetScaler Gatewayの管理］をクリックします。
3. **［追加］**をクリックし、［全般設定］で、NetScaler Gateway展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

4. 展開環境の仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。

5. 展開環境でAccess Gateway 5.0が実行されている場合は、手順9.に進みます。それ以外の場合は、必要に応じてNetScaler GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
   このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

6. NetScaler Gateway 10.1～11.0、Access Gateway 10～11.0、またはAccess Gateway 9.3のアプライアンスを追加する場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。
   - ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、［ドメインおよびセキュリティトークン］を選択します。
   - テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、［SMS認証］を選択します。
   - スマートカードを挿入してPINを入力させる場合は、［スマートカード］を選択します。

   スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、［スマートカードフォールバック］の一覧から代替の認証方法を選択します。手順2.に進みます。

7. Access Gateway 5.0のアプライアンスを追加する場合は、ユーザーのログオンポイントのホスト（スタンドアロンのアプ

ライアンスまたはクラスターの一部であるAccess Controllerサーバー）を指定します。クラスターを追加する場合は、［次へ］をクリックして手順9.に進みます。

8. NetScaler Gateway 10.1～11.0、Access Gateway 10～11.0、Access Gateway 9.3、またはスタンドアロンAccess Gateway 5.0アプライアンスを追加する場合は、［コールバックURL］ボックスにNetScaler Gateway認証サービスのURLを入力します。URLの標準的な部分は自動的に補完されます。［次へ］をクリックして手順11.に進みます。
   アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

9. StoreFrontにAccess Gateway 5.0クラスターを追加する場合は、［アプライアンス］ページでクラスター内のアプライアンスのIPアドレスまたはFQDNを一覧に追加して、［次へ］をクリックします。
10. ［サイレント認証を有効にする］ページで、Access Controllerサーバーで実行されている認証サービスのURLを一覧に追加します。一覧に複数のサーバーのURLを追加すると、その順番に基づいてフェールオーバーされます。［Next］をクリックします。
    StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

11. すべての展開環境で、XenDesktopまたはXenAppが提供するリソースをストアで使用できるようにするには、［Secure Ticket Authority（STA）］ページで、STAを実行しているサーバーのURLを一覧に追加します。一覧に複数のSTAのURLを追加すると、その順番に基づいてフェールオーバーされます。
    STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

12. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
    ［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

13. ［作成］をクリックして、NetScaler Gateway展開環境の詳細を追加します。展開環境が追加されたら、［完了］をクリックします。
    展開環境の詳細を更新する方法について詳しくは、「NetScaler Gateway接続設定の構成」を参照してください。

NetScaler Gatewayを介したストアへのアクセスを提供するには、1つの内部ビーコンポイントと、2つ以上の外部ビーコンポイントが必要です。Citrix Receiverは、ユーザーがローカルネットワークと公共のネットワークのどちらに接続しているのかをビーコンポイントを使用して識別し、適切なアクセス方法を選択します。StoreFrontでは、内部ビーコンポイントとしてデフォルトでサーバーのURLまたは負荷分散URLが使用されます。外部ビーコンポイントは、デフォルトでCitrix社のWebサイト、および管理者が追加した最初のNetScaler Gateway仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLが使用されます。ビーコンポイントの変更について詳しくは、「ビーコンポイントを構成」を参照してください。

ユーザーがNetScaler Gatewayを介してストアにアクセスできるようにするには、そのストアのリモートユーザーアクセスを構成する必要があります。

NetScaler Gatewayアプライアンスのインポート

May 22, 2017

NetScaler管理コンソールのリモートアクセス設定は、StoreFrontで構成されているものと同じように構成する必要があります。この記事では、NetScalerとStoreFrontを適切に構成して連携させるためにNetScaler Gatewayをインポートする方法について説明します。

要件

- 複数のゲートウェイ仮想サーバーをZIPファイルにエクスポートするには、NetScaler 11.1.51.21以降が必要です。**注：** NetScalerでエクスポートできるゲートウェイ仮想サーバーは、XenAppおよびXenDesktopのウィザードを使用して作成したもののみです。
- NetScalerにより生成されるZIPファイル内のGatewayConfig.jsonファイルに記載されているすべてのSTA（Secure Ticket Authority）サーバーのURLをDNSが解決でき、StoreFrontがアクセスできる必要があります。
- NetScalerで生成されるZIPファイル内のGatewayConfig.jsonファイルには、StoreFrontサーバー上にある既存のCitrix Receiver for WebサイトのURLが含まれている必要があります。バージョン11.1以降のNetScalerは、エクスポート用のZIPファイルの生成前にStoreFrontサーバーにアクセスして既存のストアとCitrix Receiver for Webサイトをすべて列挙し、この処理を自動で行います。
- StoreFrontで、インポートしたゲートウェイを使用して認証できるように、ゲートウェイVPN仮想サーバーのIPアドレスへのDNSのコールバックURLを解決できる必要があります。

  StoreFrontでゲートウェイURLを解決できる場合、使用するコールバックURLとポートの組み合わせは、通常、ゲートウェイURLとポートの組み合わせと同じものにします。

  または

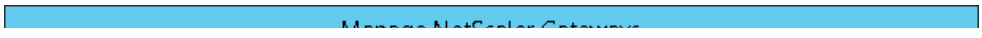
  環境内で外部と内部に違うDNS名前空間を使用する場合は、コールバックURLとポートの組み合わせをゲートウェイURLとポートの組み合わせとは異なるものにしても構いません。ゲートウェイをDMZ内に配置してのURLを使用しており、StoreFrontはプライベートの社内ネットワークに配置してのURLを使用している場合、コールバックURLを使用してDMZ内のゲートウェイ仮想サーバーへポイントバックすることができます。

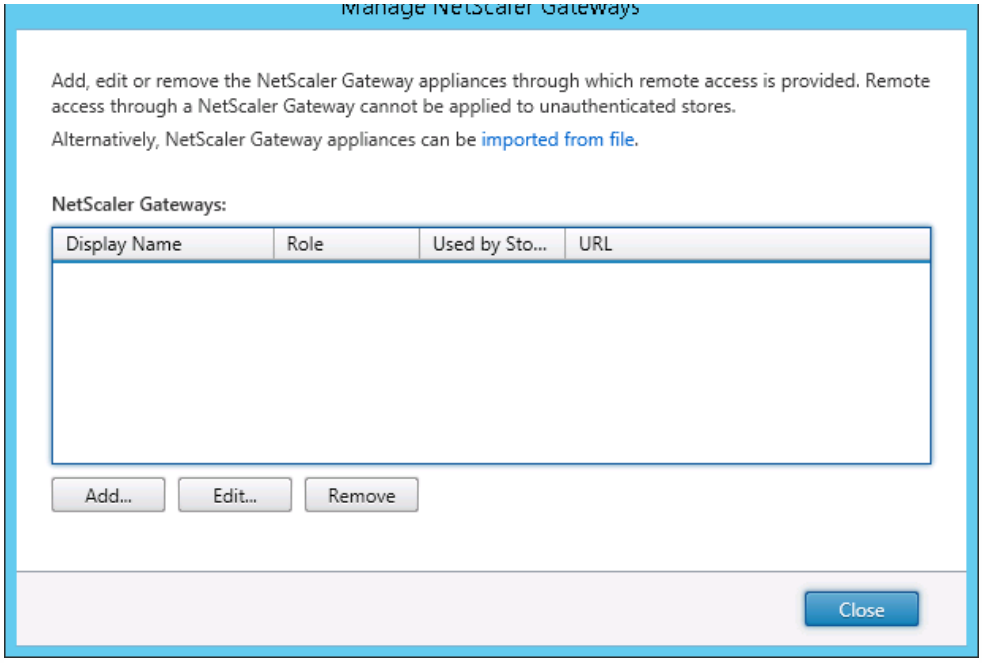
コンソールを使用してNetScaler Gatewayをインポートする

NetScaler構成ファイルをインポートすることによって、NetScaler Gatewayアプライアンスをインポートすることができます。

> **Important**
>
> 注：NetScalerからインポートされた構成ファイルを手で編集することはできません。

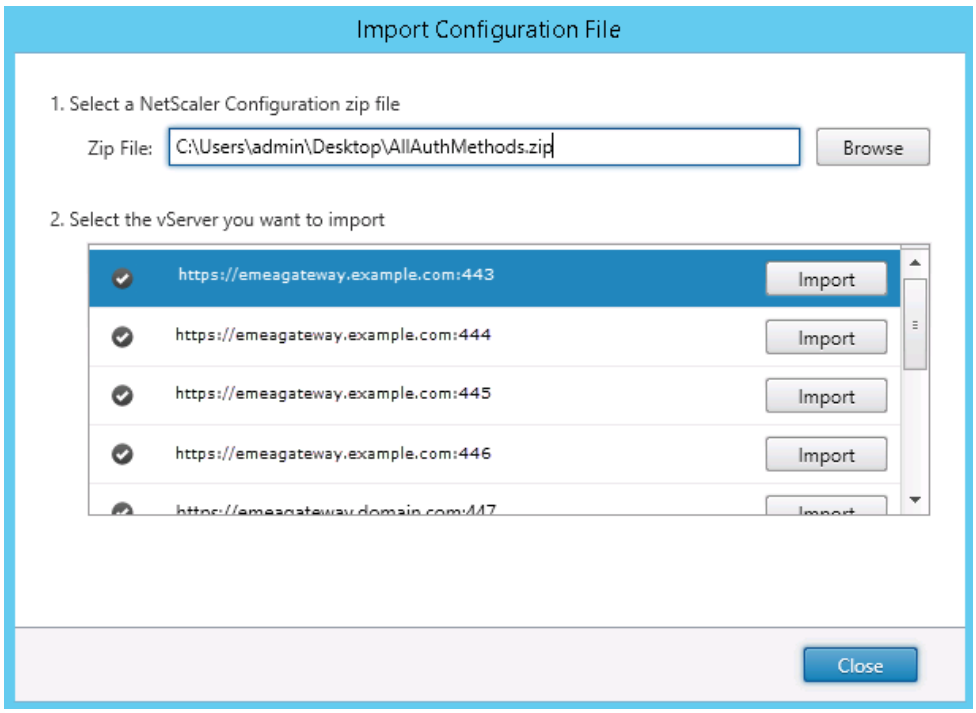
1. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、 **[操作]** ペインの **[NetScaler Gatewayの管理]** をクリックします。
2. ［NetScaler Gatewayの管理］画面で、 **[ファイルからインポート]** リンクをクリックします。





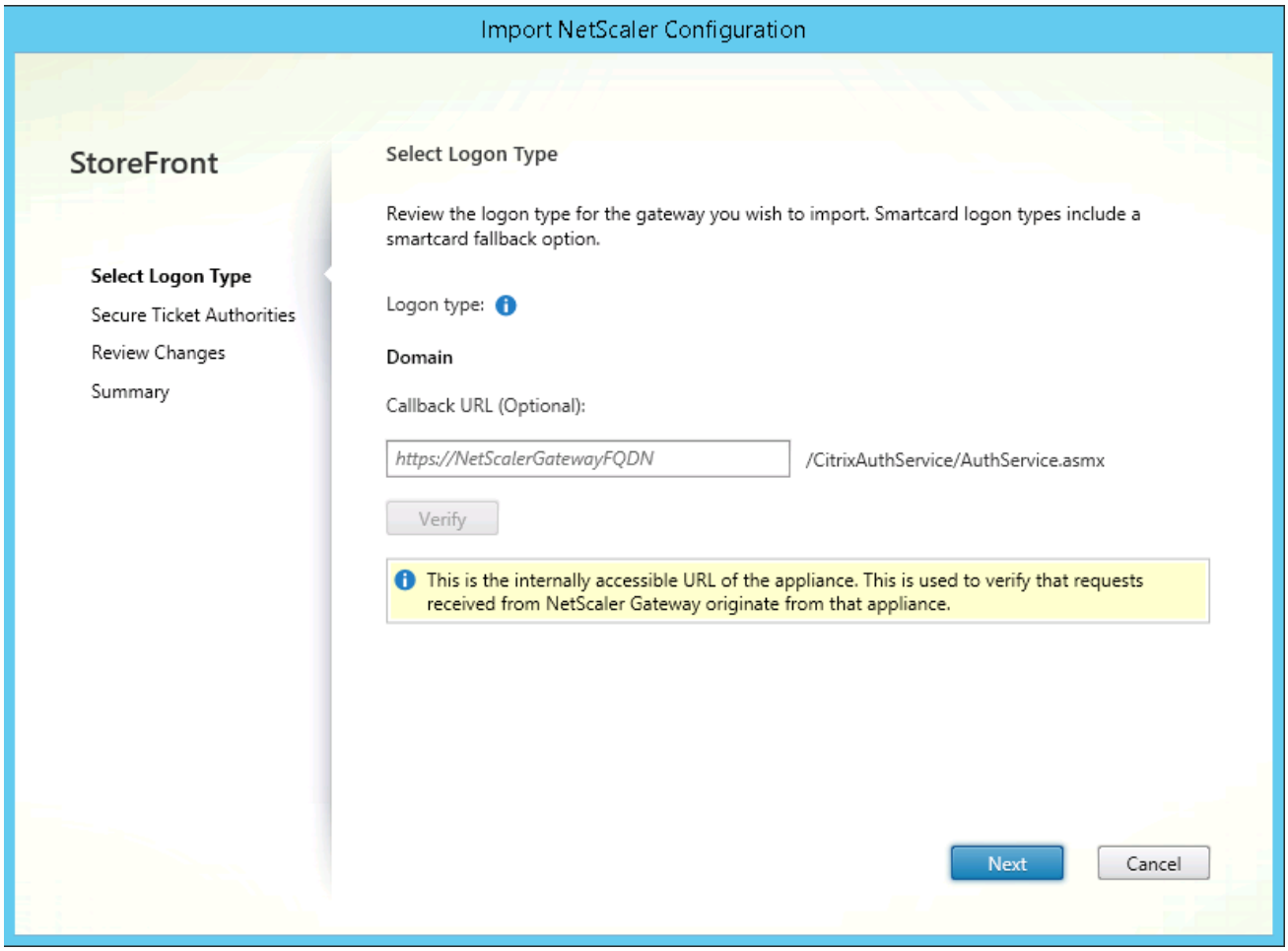
3. 1. NetScaler 構成の zip ファイルを選択してください

4. 選択したZIPファイルに含まれるゲートウェイ仮想サーバーの一覧が表示されます。インポートするゲートウェイ仮想サーバーを選択し、 **[インポート]** をクリックします。仮想サーバーを繰り返してインポートする場合、［インポート］ボタンは［更新］ボタンになります。 **[更新]** をクリックした場合、後でゲートウェイを上書きするか新規に作成することができます。



5. 選択したゲートウェイのログオンの種類を確認し、必要に応じてコールバックURLを指定します。［ログオンの種類］の一覧から、Citrix Receiverユーザー向けにアプライアンス上で構成した認証方法を選択します。ログオンの種類によってはコールバックURLが必要になります（表を参照）。

- **[確認]** をクリックして、コールバックURLが有効でありStoreFrontサーバーから到達可能であることをチェックします。



コンソールでの［ログオンの種類］	JSONファイルでのLogonType	ｺｰﾙﾊﾞｯｸ URL(必須)(_U):
ドメイン	ドメイン	なし
ドメインおよびセキュリティ トークン	DomainAndRSA	なし
セキュリティトークン	RSA	はい
スマートカード - フォールバックがありません	スマートカードの使用	はい
スマートカード - ドメイン	SmartCardDomain	はい
スマートカード - ドメインおよびセキュリティ トークン	SmartCardDomainAndRSA	はい

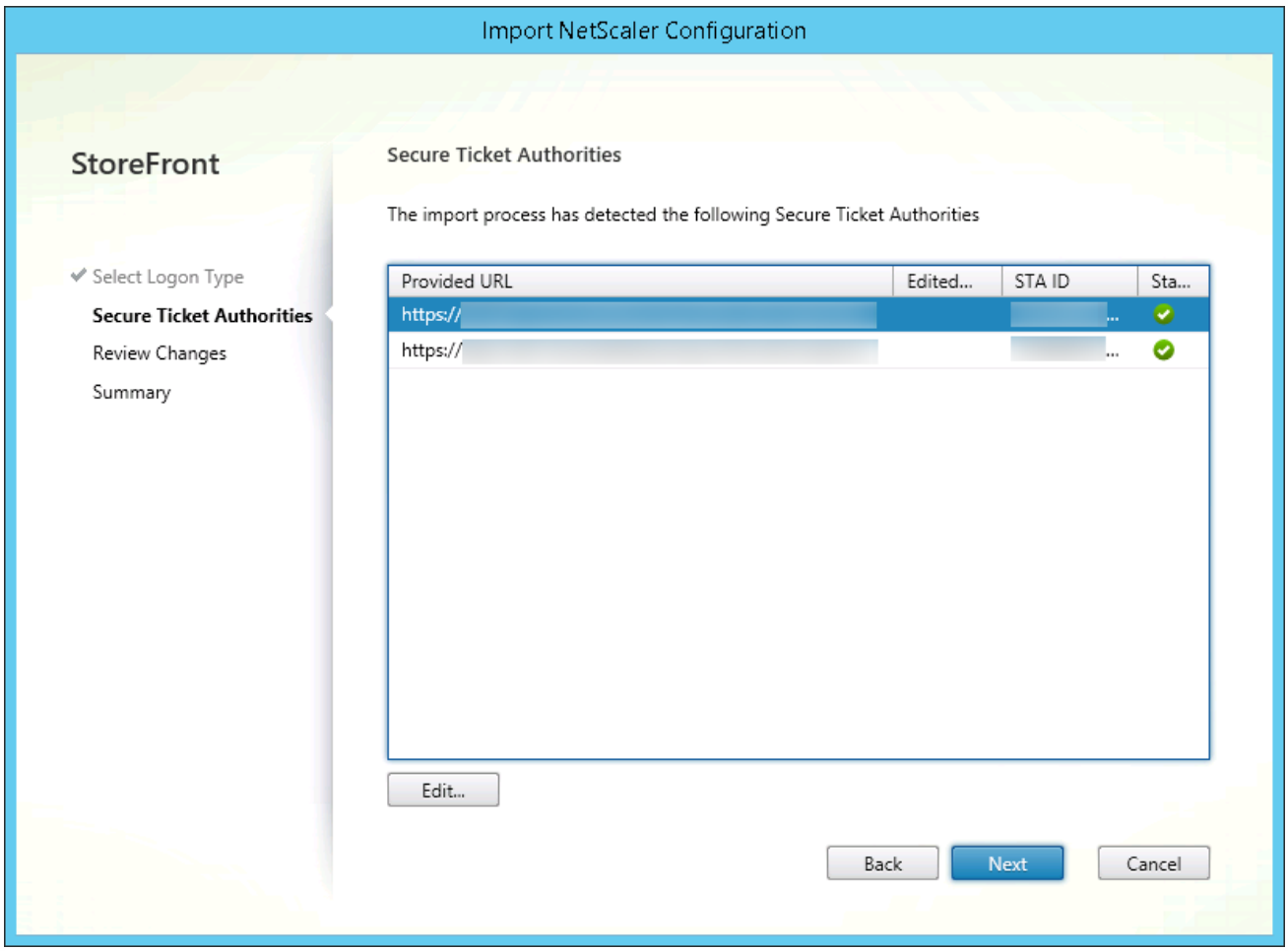
スマートカード - セキュリティ トークン	SmartCardRSA	はい
スマートカード - SMS 認証	SmartCardSMS	はい
SMS 認証	SMS：	はい

コールバックURLが必要な場合、ZIPファイルに記載されているゲートウェイURLに基づいてStoreFrontによりコールバックURLが自動で入力されます。このURLは、NetScaler Gateway仮想サーバーのIPにポイントバックする有効なURLに変更できます。

スマートアクセスを使用する場合、コールバックURLは必須です。

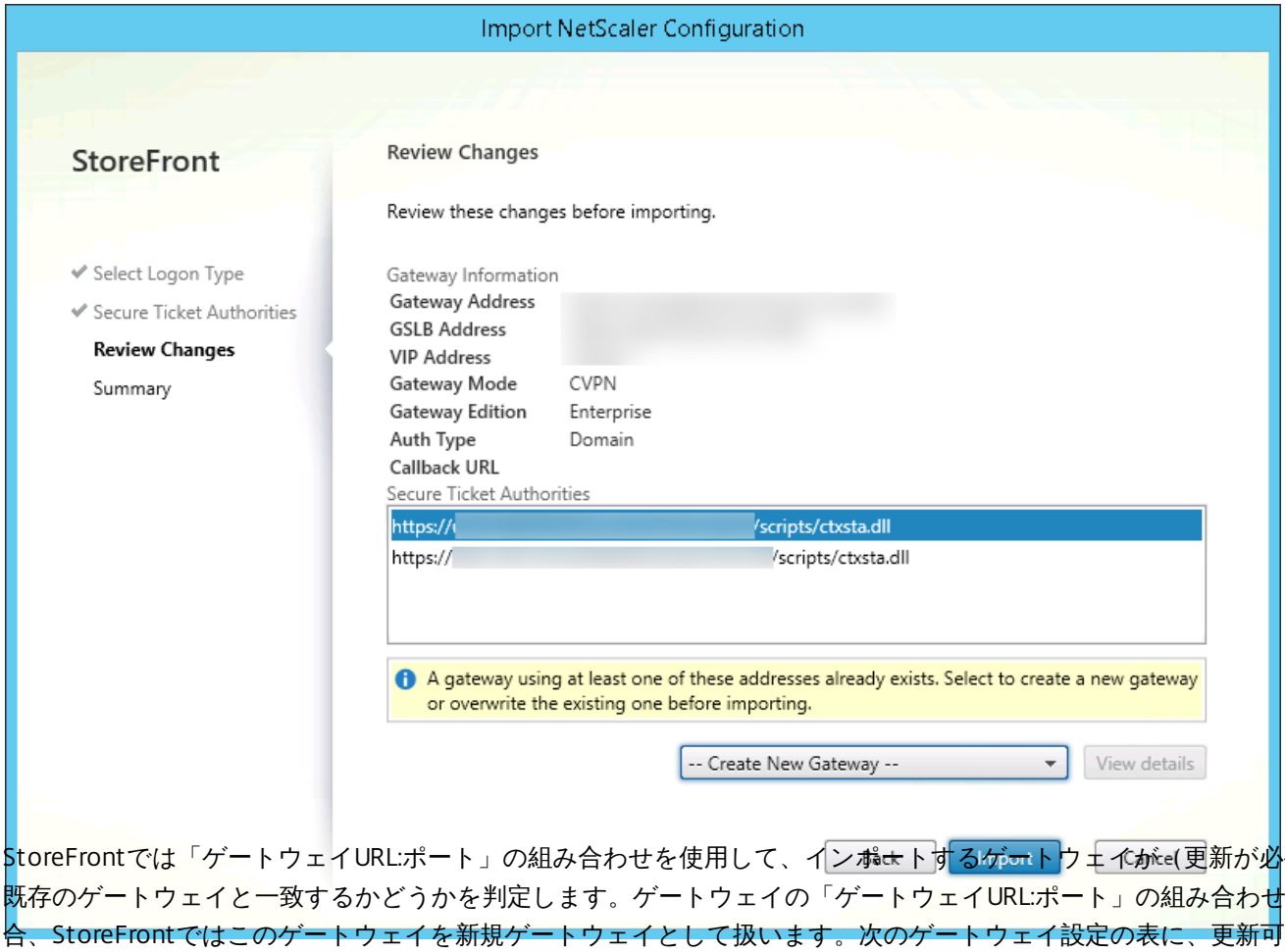
6. **[Next]** をクリックします。

7. StoreFrontが、ZIPファイルに記載されているすべてのSTA（Secure Ticket Authority）サーバーのURLへDNSを使用してアクセスし、これらのサーバーが動作中のSTAチケット発行サーバーであることを確認します。いずれかのSTA URLが無効である場合、インポートは中断されます。



8. **[Next]** をクリックします。

9. インポートの詳細を確認します。ゲートウェイURLとポートの組み合わせ（ゲートウェイ:ポート）の同じゲートウェイが既に存在する場合は、ボックスの一覧からゲートウェイを選択して上書きするか、新規ゲートウェイを作成します。



StoreFrontでは「ゲートウェイURL:ポート」の組み合わせを使用して、インポートするゲートウェイが（更新が必要になる）既存のゲートウェイと一致するかどうかを判定します。ゲートウェイの「ゲートウェイURL:ポート」の組み合わせが異なる場合、StoreFrontではこのゲートウェイを新規ゲートウェイとして扱います。次のゲートウェイ設定の表に、更新可能な設定を示します。

ゲートウェイの設定	更新の可否
「ゲートウェイURL:ポート」の組み合わせ	なし
GSLBのURL	はい
Netscalerの信頼証明書と捺印	はい
コールバック URL	はい
Receiver for WebサイトのURL	はい
ゲートウェイのアドレス/VIP	はい
STAのURLおよびSTAのID	はい
すべてのログオンの種類	はい

10. [**Import**] をクリックします。StoreFrontサーバーがサーバーグループに含まれている場合、インポートしたゲートウェイ設定をグループ内の他のサーバーに反映させるように求めるメッセージが表示されます。

11. [**完了**] をクリックします。

別の仮想サーバー構成をインポートする場合は、上記の手順を繰り返します。

> ### 注意
>
> 別のゲートウェイを使用するようにネイティブCitrix Receiverを構成していない場合、ストアのデフォルトゲートウェイが、ネイティブCitrix Receiverが接続に使用するゲートウェイとなります。ストアのゲートウェイが構成されていない場合、ZIPファイルからインポートされた1番目のゲートウェイが、ネイティブCitrix Receiverが使用するデフォルトゲートウェイになります。後でゲートウェイをインポートしても、ストアに設定済みのデフォルトゲートウェイは変更されません。

PowerShellを使用して複数のNetScaler Gatewayをインポートする

Read-STFNetScalerConfiguration

- 現在ログオンしているStoreFront管理者のデスクトップにZIPファイルをコピーします。
- NetScalerのZIPファイルの内容をメモリに読み込み、インデックス値を使用してファイルに含まれる3つのゲートウェイを確認します。

```
-command                                                                                                    コピー

$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Read-STFNetScalerConfigurationコマンドレットを使用して、NetscalerのZIPインポートパッケージからメモリ内に読み込んだ3つのゲートウェイオブジェクトを表示します。

```
-command                                                                                                    コピー

$ImportedGateways.Document.Gateways[0]

$ImportedGateways.Document.Gateways[1]

$ImportedGateways.Document.Gateways[2]



GatewayMode          : CVPN
```

```
CallbackUrl           :

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:443

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.1

Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       : Domain

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode           : CVPN

CallbackUrl           :

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:444

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.2
```

```
Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       : DomainAndRSA

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode           : CVPN

CallbackUrl           : https://emeagateway.example.com:445

GslbAddressUri        : https://gslb.example.com/

AddressUri            : https://emeagateway.example.com/

Address               : https://emeagateway.example.com:445

GslbAddress           : https://gslb.example.com:443

VipAddress            : 10.0.0.2

Stas                  : {STA298854503, STA909374257}

StaLoadBalance        : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType       :SmartCard

GatewayEdition        : Enterprise

ReceiverForWebSites   : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}
```

コールバックURLを指定せずにImport-STFNetScalerConfigurationを使用する

現在ログインしているStoreFront管理者のデスクトップにZIPファイルをコピーします。 NetScalerのZIPインポートパッケージをメモリに読み込み、インデックス値を使用してファイルに含まれる3つのゲートウェイを確認します。

```
-command
```
コピー

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Import-STFNetScalerConfigurationコマンドレットを使用し、必要なゲートウェイインデックスを指定してStoreFrontに新しい3つのゲートウェイをインポートします。 -Confirm:$Falseパラメーターを使用することで、Powershell GUIからゲートウェイのインポートを1つ1つ許可するように求められなくなります。 1度に1つのゲートウェイをインポートする場合、このパラメーターは削除してください。

```
-command
```
コピー

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -Confirm:$False
```

独自のコールバックURLを指定してImport-STFNetScalerConfigurationを使用する

Import-STFNetScalerConfigurationコマンドレットと-CallbackUrlパラメーターを使用し、任意のコールバックを指定して3つの新しいゲートウェイをStoreFrontへインポートします。

```
-command
```
コピー

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.co

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.co

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.co
```

Import-STFNetScalerConfigurationを使用してインポートファイルに格納されている認証方法を上書きし独自のコールバックURLを指定する

- Import-STFNetScalerConfigurationコマンドレットと-CallbackUrlパラメーターを使用し、任意のコールバックを指定して3つの新しいゲートウェイをStoreFrontへインポートします。

```
-command                                                                                                    コピー

$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://em

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://em

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://em
```

NetScaler Gateway接続設定の構成

May 22, 2017

以下のタスクでは、ユーザーがストアにアクセスするときに経由するNetScaler Gateway環境の詳細を更新します。StoreFrontでのWebFront Gatewayの構成について詳しくは、「Using WebFront to Integrate with StoreFront」を参照してください。

NetScaler Gateway環境の構成を変更する場合は、そのNetScaler Gatewayを経由してストアにアクセスするユーザーに変更内容を通知して、Citrix Receiverの設定を更新させてください。ストアのCitrix Receiver for Webサイトが構成済みの場合、ユーザーはそのサイトから最新のCitrix Receiverプロビジョニングファイルを入手できます。Receiver for Webサイトが構成済みでない場合は、管理者がストアのプロビジョニングファイルをエクスポートしてユーザーに提供します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

NetScaler Gatewayの全般的な設定の変更

ユーザーに表示されるNetScaler Gateway環境の名前を変更し、NetScaler Gatewayインフラストラクチャの仮想サーバー、ユーザーログオンポイントのURL、および展開モードを変更するには、［全般設定の変更］タスクを使用します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、［NetScaler Gatewayの管理］をクリックします。
3. NetScaler Gatewayの展開環境にわかりやすい名前を指定します。
   ここで指定する表示名がユーザーのCitrix Receiverに表示されます。そのため、ユーザーが使用するNetScaler Gatewayを判断しやすいように、名前に関連情報を含める必要があります。たとえば、ユーザーが自分のいる場所に最も便利なNetScaler Gatewayを簡単に特定できるように、表示名に地理情報を含めることができます。

4. 展開環境の仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLを入力します。展開環境で使用する製品のバージョンを指定します。
   StoreFront展開環境のFQDN（Fully Qualified Domain Name：完全修飾ドメイン名）は一意で、NetScaler Gateway仮想サーバーのFQDNと異なるものである必要があります。StoreFrontとNetScaler Gateway仮想サーバーに同じFQDNを使用することはサポートされていません。

5. 展開環境でAccess Gateway 5.0が実行されている場合は、手順7.に進みます。それ以外の場合は、必要に応じてNetScaler GatewayアプライアンスのサブネットIPアドレスを指定します。サブネットIPアドレスは、Access Gateway 9.3アプライアンスの場合は必須ですが、それより後の製品バージョンではオプションです。
   このサブネットアドレスは、NetScaler Gatewayで内部ネットワークのサーバーと通信するときに、ユーザーデバイスを表すために使用するIPアドレスです。このアドレスは、NetScaler GatewayアプライアンスのマップされたIPアドレスである場合もあります。StoreFrontは、サブネットIPアドレスを使用して、受信要求が信頼されているデバイスから発信されているかどうかを検証します。

6. アプライアンスでNetScaler Gateway 10.1 - 11.0、Access Gateway 10 - 11.0、またはAccess Gateway 9.3を実行している場合は、［ログオンの種類］の一覧から、Citrix Receiverユーザー用にアプライアンスで構成した認証方法を選択します。
   NetScaler Gatewayアプライアンスに関する構成情報は、ストアのプロビジョニングファイルに追加されます。これにより、Citrix Receiverは、アプライアンスへの初回接続時に適切な接続要求を送信できるようになります。

   - ユーザーのMicrosoft Active Directoryドメインの資格情報を入力させる場合は、［ドメイン］を選択します。
   - セキュリティトークンから取得するトークンコードを入力させる場合は、［セキュリティトークン］を選択します。

- ユーザーのドメイン資格情報とセキュリティトークンから取得するトークンコードの両方を入力させる場合は、[ドメインおよびセキュリティトークン]を選択します。
- テキストメッセージで送信されるワンタイムパスワードを入力させる場合は、[SMS認証]を選択します。
- スマートカードを挿入してPINを入力させる場合は、[スマートカード]を選択します。

スマートカードでの認証に問題が生じた場合に代替の認証方法を使用できるようにするには、[スマートカードフォールバック]の一覧から代替の認証方法を選択します。

7. 展開環境でNetScaler Gateway 10.1～11.0、Access Gateway 10～11.0、Access Gateway 9.3、または単一のAccess Gateway 5.0アプライアンスを実行している場合は、NetScaler Gateway認証サービスのURLを［コールバックURL］ボックスに入力します。URLの標準的な部分は自動的に補完されます。
   アプライアンスの内部URLを入力します。StoreFrontはNetScaler Gateway認証サービスに接続して、NetScaler Gatewayからの要求の送信元がそのアプライアンスであることを確認します。

Access Gateway 5.0アプライアンスの管理

StoreFrontでAccess Gateway 5.0クラスター内のアプライアンスのIPアドレスまたはFQDNを追加、編集、または削除するには、［アプライアンスの管理］タスクを使用します。

Access Controllerを経由するサイレントユーザー認証の有効化

Access Gateway 5.0クラスターのAccess Controllerサーバーで実行している認証サービスのURLを追加、編集、または削除するには、［サイレント認証を有効にする］タスクを使用します。一覧に複数のサーバーのURLを入力すると、その順番に基づいてフェールオーバーされます。StoreFrontでは認証サービスを使用してリモートユーザーが認証されるため、リモートユーザーがストアにアクセスするときに資格情報を再入力する必要はありません。

Secure Ticket Authorityの管理

ユーザーセッションチケットを取得するSecure Ticket Authority（STA）の一覧を更新したり、セッション画面の保持機能を構成したりするには、［Secure Ticket Authority］タスクを使用します。STAは、XenDesktopおよびXenAppサーバーでホストされ、接続要求に応答してセッションチケットを発行します。セッションチケットは、XenDesktopおよびXenAppリソースへのアクセスを認証および承認するための基本機能です。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで［ストア］ノードを選択して、結果ペインでNetScaler Gateway展開環境を選択します。［操作］ペインの［NetScaler Gatewayの管理］をクリックします。
3. ［追加］をクリックして、STAサーバーのURLを入力します。一覧に複数のSTAのURLを入力すると、その順番に基づいてフェールオーバーされます。URLを変更するには、［Secure Ticket Authority URL］ボックスの一覧でエントリを選択して［編集］をクリックします。特定のSTAからセッションチケットを取得しないようにするには、一覧でURLを選択して［削除］をクリックします。
4. Citrix Receiverが自動的に再接続を実行する間に、切断したセッションをXenDesktopおよびXenAppで開いたままにするには、［セッション画面の保持を有効にする］チェックボックスをオンにします。複数のSTAを構成した環境でセッション画面の保持機能を常に使用できるようにするには、［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにします。
   ［可能な場合は2つのSTAにチケットを要求する］チェックボックスをオンにすると、セッションの途中で1つのSTAが使用できなくなってもユーザーセッションが中断されないように、StoreFrontにより2つの異なるSTAからセッションチケットが取得されます。StoreFrontがどちらのSTAにもアクセスできない場合は、単一のSTAを使用するようにフォールバックされます。

NetScaler Gateway展開環境の削除

［操作］ペインで、**［NetScaler Gatewayの管理］**の［削除］タスクを使用して、NetScaler Gateway展開環境の詳細を

StoreFrontから削除します。NetScaler Gateway環境を削除すると、ユーザーはその展開環境を経由してストアにアクセスてきなくなります。

NetScalerによる負荷分散

May 22, 2017

ここでは、負荷分散用にNetScalerを使用するために必要な情報について示します。

StoreFrontサーバーグループとNetScaler負荷分散の構成

NetScaler負荷分散およびStoreFrontサーバーに対するSSL証明書の作成

サーバーグループ間のサブスクリプション同期用負荷分散仮想サーバーの作成

負荷分散用StoreFrontサーバーグループの構成

Citrixサービスモニター

同じNetScaler Gatewayアプライアンス上のNetScaler Gatewayおよび負荷分散仮想サーバー

NetScalerを使ってStoreFrontサーバーグループを負荷分散する場合のループバックオプション

StoreFrontサーバーグループとNetScaler負荷分散の構成

負荷分散StoreFrontの展開計画

ここでは、すべてのアクティブな負荷分散構成に2つ以上のStoreFrontサーバーを含むStoreFrontサーバーグループを展開する方法について説明します。また、サーバーグループのすべてのStoreFrontノード間でCitrix Receiver/Citrix Receiver for Webからの受信要求を負荷分散するため、NetScalerアプライアンスを構成する方法と、NetScalerまたはサードパーティのロードバランサーで使用するため新しいStoreFrontモニターを構成する方法について詳しく説明します。

負荷分散構成の例については、後述の「シナリオ1」と「シナリオ2」を参照してください。

テストされた環境

- 単一のサーバーグループ内の4つのWindows Server 2012 R2 StoreFront 3.0ノード。
- 最小接続およびCookieInsert “sticky”負荷分散用に構成された1つのNetScaler 10.5ロードバランサー。
- Fiddler 4.0およびCitrix Receiver for Windows 4.3がインストールされた1つのWindows 8.1テストクライアント。

HTTPSを使用する場合に負荷分散化される展開のSSL証明書要件

「ゲートウェイとサーバー証明書の使用方法の計画」セクションを参照してください。

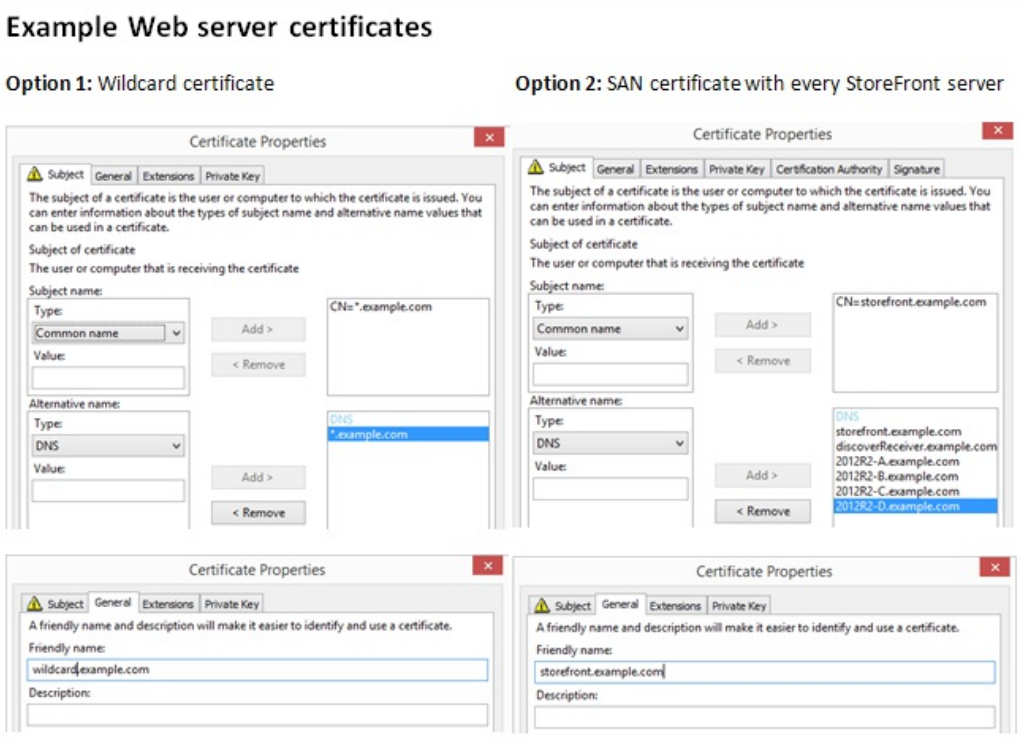
商用証明機関から証明書を購入する、またはエンタープライズCAから発行しようとする前に、次のオプションについて検討します。

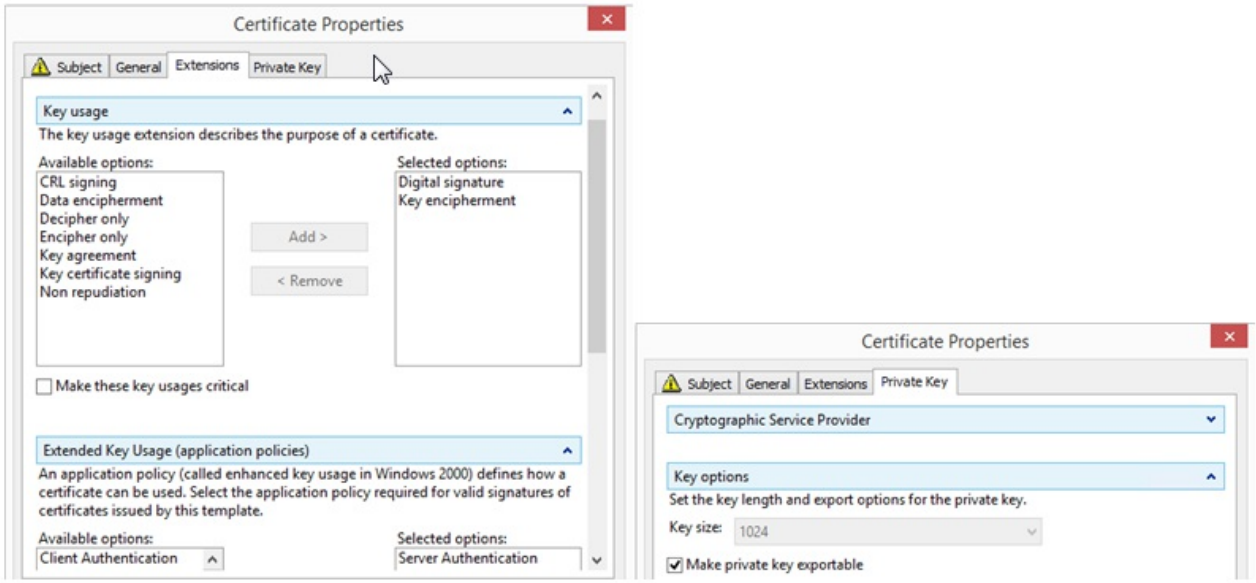
- **オプション1：** *.example.comワイルドカード証明書をNetScaler負荷分散仮想サーバーとStoreFrontサーバーグループノードの両方で使用する。これにより構成が簡素化され、将来的には証明書を置き換える必要なく追加のStoreFrontサーバーを増やすことができます。
- **オプション2：** サブジェクトの別名（SAN）が含まれている証明書をNetScaler負荷分散仮想サーバーとStoreFrontサーバーグループノードの両方で使用する。すべてのStoreFrontサーバーの完全修飾ドメイン名（FQDN）と一致する証明書内の追加のSANはオプションですが、これによりStoreFront展開環境に柔軟性がもたらせられるため、推奨されます。メールベースの検出discoverReceiver.example.com用のSANを含めます。

  メールベースの検出の構成については、http://blogs.citrix.com/2013/04/01/configuring-email-based-account-

discovery-for-citrix-receiver/を参照してください。

注： 証明書に関連付けられている秘密キーをエクスポートできない場合は、注：エクスポートする場合、証明書に割り当てられている秘密キーは実行できません。NetScaler負荷分散仮想サーバー上の証明書と、StoreFrontサーバーグループノードの証明書という2つの別個の証明書を使用します。どちらの証明書にもサブジェクトの別名が必要です。





NetScaler負荷分散およびStoreFrontサーバーに対するSSL証明書の作成

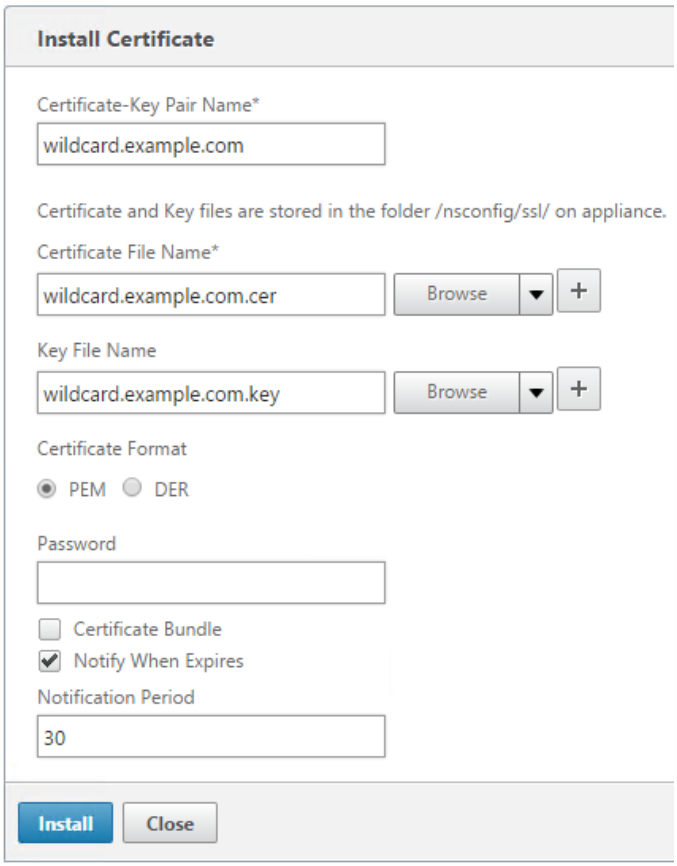
OpenSSLを使った、Windows CAから発行された証明書のNetaScalerアプライアンスへのインポート

- WinSCPは、WindowsマシンからNetScalerファイルシステムへのファイル移動に役立つ無料のサードパーティ製ツールです。インポートする証明書を、NetScalerファイルシステム内の**/nsconfig/ssl/**フォルダーにコピーします。
- また、NetScaler上でOpenSSLツールを使用して、**PKCS12/PFX**ファイルから証明書とキーを抽出し、NetScalerで使用できるPEM形式で、2つの別々のCERファイルとKEY X.509ファイルを作成することができます。

1. このPFXファイルをNetScaler GatewayアプライアンスまたはVPXの**/nsconfig/ssl**にコピーします。
2. NetScalerコマンドラインインターフェイス（CLI）を開きます。
3. 「**Shell**」と入力してNetScaler CLIを閉じ、FreeBSDシェルに切り替えます。
4. ディレクトリを変更するために、「**cd /nsconfig/ssl**」と入力します。
5. **openssl pkcs12 -in .pfx -nokeys -out .cer**を実行し、画面のメッセージに従ってPFXパスワードを入力します。
6. **openssl pkcs12 -in .pfx -nocerts -out .key**を実行し、画面のメッセージに従ってPFXパスワードを入力して、次に秘密キーのPEMパスフレーズを設定してKEYファイルを保護します。
7. **ls –al**を実行し、**/nsconfig/ssl/**内にCERファイルとKEYファイルが正常に作成されたことを確認します。
8. 「**Exit**」と入力してNetScaler CLIに戻ります。

インポート後にNetScalerでSSL証明書の構成

1. NetScaler管理GUIにログオンします。
2. ［Traffic Management］>［SSL］>［SSL Certificates］の順に選択し、［Install］をクリックします。
3. ［Install Certificate］ウィンドウで証明書と秘密キーペア名を入力します。
   - o NetScalerファイルシステムの/nsconfig/ssl/で.cer証明書ファイルを選択します。
   - o 同じ場所から秘密キーを含む.keyファイルを選択します。



StoreFrontサーバーグループ負荷分散用のDNSレコードの作成

選択した共用FQDN用にDNS AおよびPTRレコードを作成します。ネットワーク内のクライアントはこのFQDNを使用して、ロードバランサーを使用するStoreFrontサーバーにアクセスします。

例 - **storefront.example.com**が仮想サーバー仮想IP（VIP）の負荷分散を解決。

シナリオ1：クライアントとNetScalerロードバランサー間、またNetScalerロードバランサーと2つ以上のStoreFront 3.0サーバー間のエンドツーエンドのHTPPS 443セキュア接続。

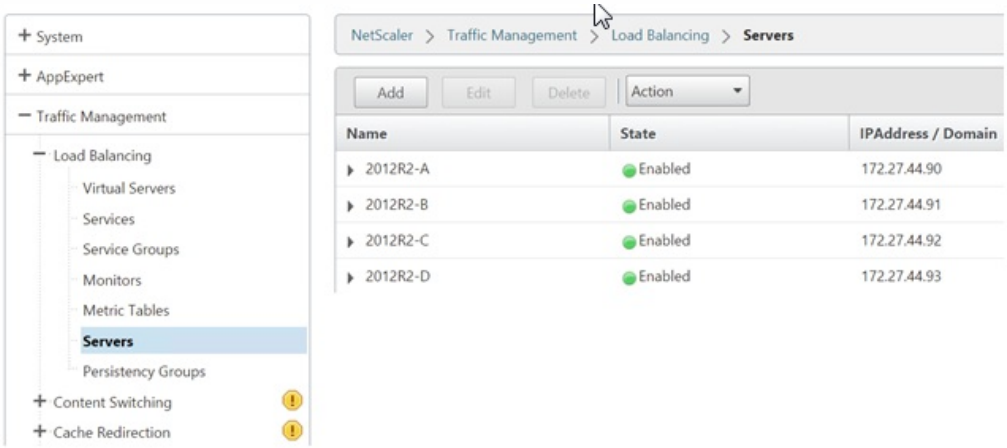
このシナリオでは、ポート443を使用する変更されたStoreFrontモニターが使用されます。

個々のStoreFrontサーバーノードのNetScalerロードバランサーへの追加

1. NetScaler管理GUIにログオンします。
2. **［Traffic Management］>［負荷分散］>［サーバー］>［追加］**の順に選択し、4つのStoreFrontノードをそれぞれ追加して負荷分散させます。

   例 = 4 x 2012R2 StoreFront Nodes called 2012R2-A to –D

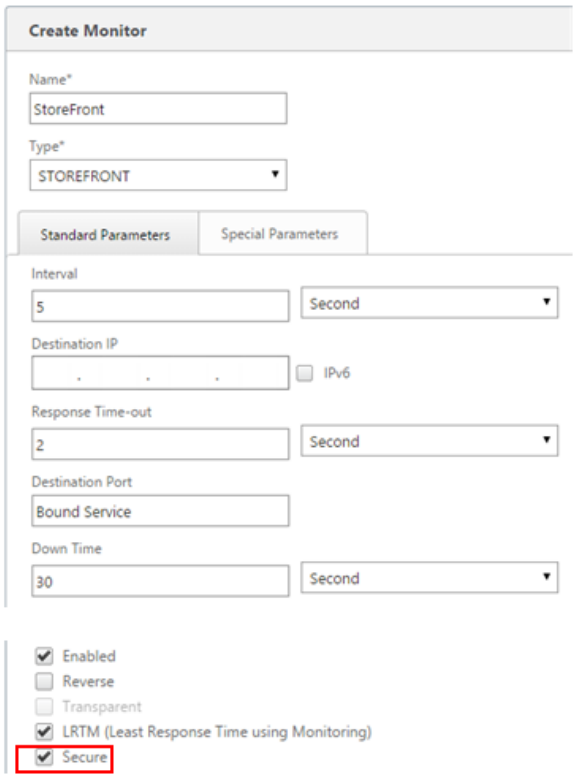
3. IPベースのサーバー構成を使用し、各StoreFrontノードのサーバーIPアドレスを入力します。



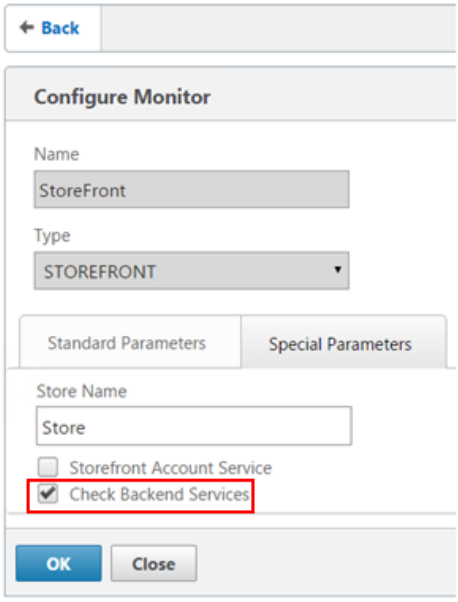
StoreFrontモニターを定義して、サーバーグループ内のすべてのStoreFrontノードをチェックします。

1. NetScaler管理GUIにログオンします。
2. **［Traffic Management］>［負荷分散］>［モニター］>［追加］**の順に選択し、StoreFrontを呼び出す新しいモニターを追加してすべてのデフォルト設定を受け入れます。
3. **［Type］**ドロップダウンの一覧から**［StoreFront］**を選択します。
4. 負荷分散仮想サーバーとStoreFront間でSSL接続を使用している場合は、**［Secure］**チェックボックスをオンにする必要があります。その他の場合はオフのままにします。
5. ［Special Parameters］タブでストア名を指定します。
6. ［Special Parameters］タブで**［Check Backend Services］**チェックボックスをオンにします。このオプションにより、StoreFrontサーバーで監視サービスの実行が有効になります。StoreFrontサーバーで実行するWindowsサービスをプローブしてStoreFrontサービスが監視され、実行中のすべてのStoreFrontサービスの状態が返されます。

Standard Parameters Tab



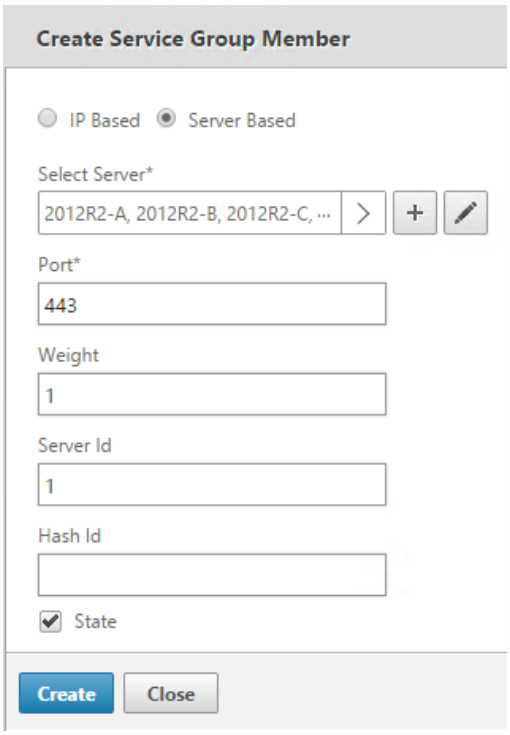
Special Parameters Tab



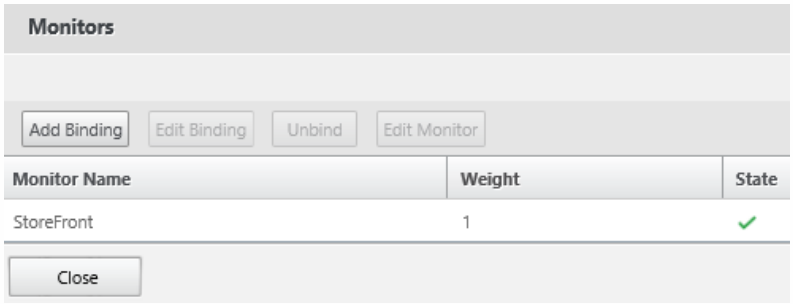
すべてのStoreFrontサーバーを含むHTTPS 443サービスグループの作成

1. サービスグループ内で、右側の［Members］オプションを選択し、サーバーセクションで以前定義したすべてのStoreFrontサーバーノードを追加します。

2. SSLポートを設定し、各ノードに一意のサーバーIDを追加します。

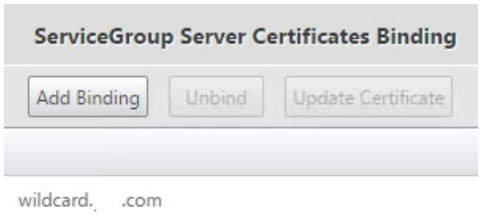


3. ［Monitors］タブで前に作成したStoreFrontモニターを選択します。



4. ［Certificates］タブで、前にインポートしたSSL証明書をバインドします。

5. 以前にインポートしたSSL証明書の署名に使用されたCA証明書とPKIチェーン信頼の一部の可能性があるそのほかのCAをバインドします。

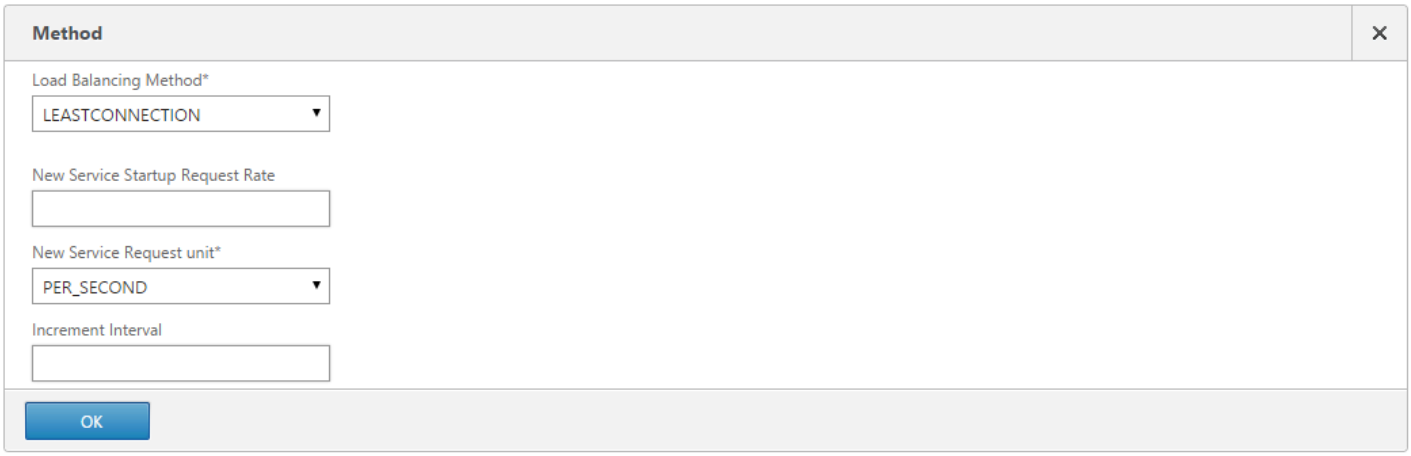


ユーザートラフィック用負荷分散仮想サーバーの作成

1. NetScaler管理GUIにログオンします。

2. **［Traffic Management］ > ［負荷分散］ > ［仮想サーバー］ > ［追加］**の順に選択し、新しい仮想サーバーを作成します。

3. 仮想サーバー用の負荷分散方式を選択します。StoreFront負荷分散で共通の選択は、［**round robin**］または［**least connection**］です。



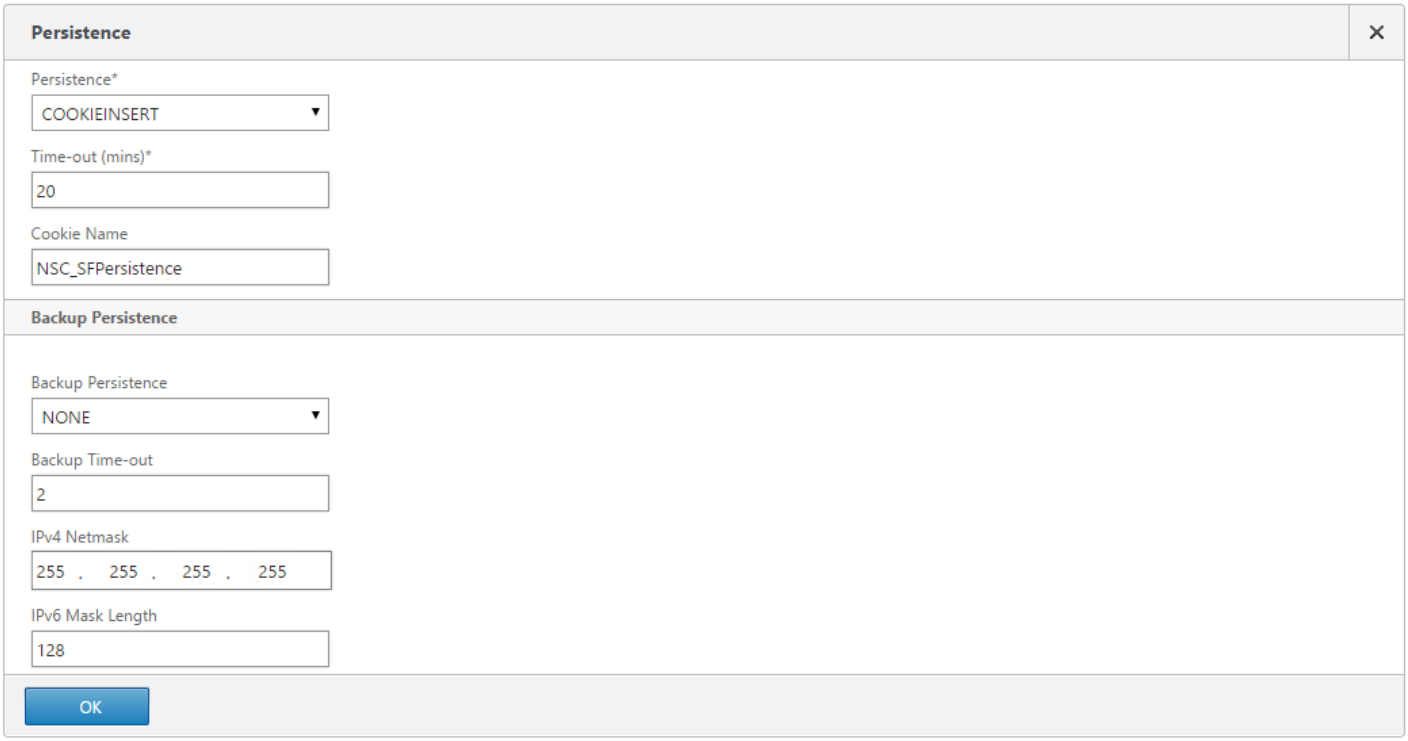
4. 前に作成した**Service Group**を負荷分散仮想サーバーにバインドします。

5. 以前にサービスグループにバインドしたのと同じSSLおよびCA証明書を負荷分散仮想サーバーにバインドします。

6. 負荷分散仮想サーバーメニュー内から、右側にある［**Persistence**］を選択して、パーシステンス方式が**CookieInsert**になるように設定します。

7. cookieに名前を付けます。たとえば、デバッグ時にFiddlerトレースで見つけやすいように**NSC_SFPersistence**という名前を付けます。

8. バックアップパーシステンスを［**None**］に設定します。



シナリオ2：SSL終了 - クライアントとNetScalerロードバランサー間のHTTPS 443通信、およびロードバランサーとその裏のStoreFront 3.0サーバー間のHTTP 80 接続。

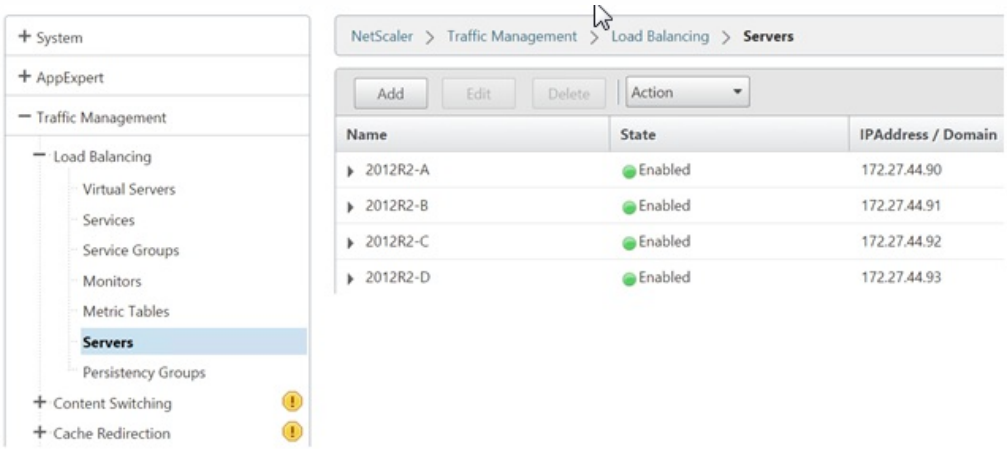
このシナリオでは、ポート8000を使用するデフォルトのStoreFrontモニターが使用されます。

個々のStoreFrontサーバーのNetScalerロードバランサーへの追加

1. NetScaler管理GUIにログオンします。
2. **［Traffic Management］>［負荷分散］>［サーバー］>［追加］**の順に選択し、4つのStoreFrontサーバーをそれぞれ追加して負荷分散させます。

   例 = 4 x 2012R2 Storefront servers called 2012R2-A to -D

3. IPベースのサーバー構成を使用し、各StoreFrontサーバーのサーバーIPアドレスを入力します。



HTTP 8000 StoreFrontモニターを定義して、サーバーグループ内のすべてのStoreFrontサーバーをチェックします。

1. NetScaler管理GUIにログオンします。
2. **［Traffic Management］>［Monitors］>［Add］**の順に選択し、StoreFrontを呼び出す新しいモニターを追加します。
3. 新しいモニターの名前を入力し、すべてのデフォルトの設定を受け入れます。
4. **［Type］**ドロップダウンメニューから**［StoreFront］**を選択します。
5. ［Special Parameters］タブでストア名を指定します。
6. ポートに「**8000**」を入力して、各StoreFrontサーバーで作成されるデフォルトのモニターインスタンスと一致させます。
7. ［Special Parameters］タブで**［Check Backend Services］**チェックボックスをオンにします。このオプションにより、StoreFrontサーバーで監視サービスの実行が有効になります。StoreFrontサーバーで実行するWindowsサービスをプローブしてStoreFrontサービスが監視され、実行中のすべてのStoreFrontサービスの状態が返されます。

すべてのStoreFrontサーバーを含むHTTP 80サービスグループの作成

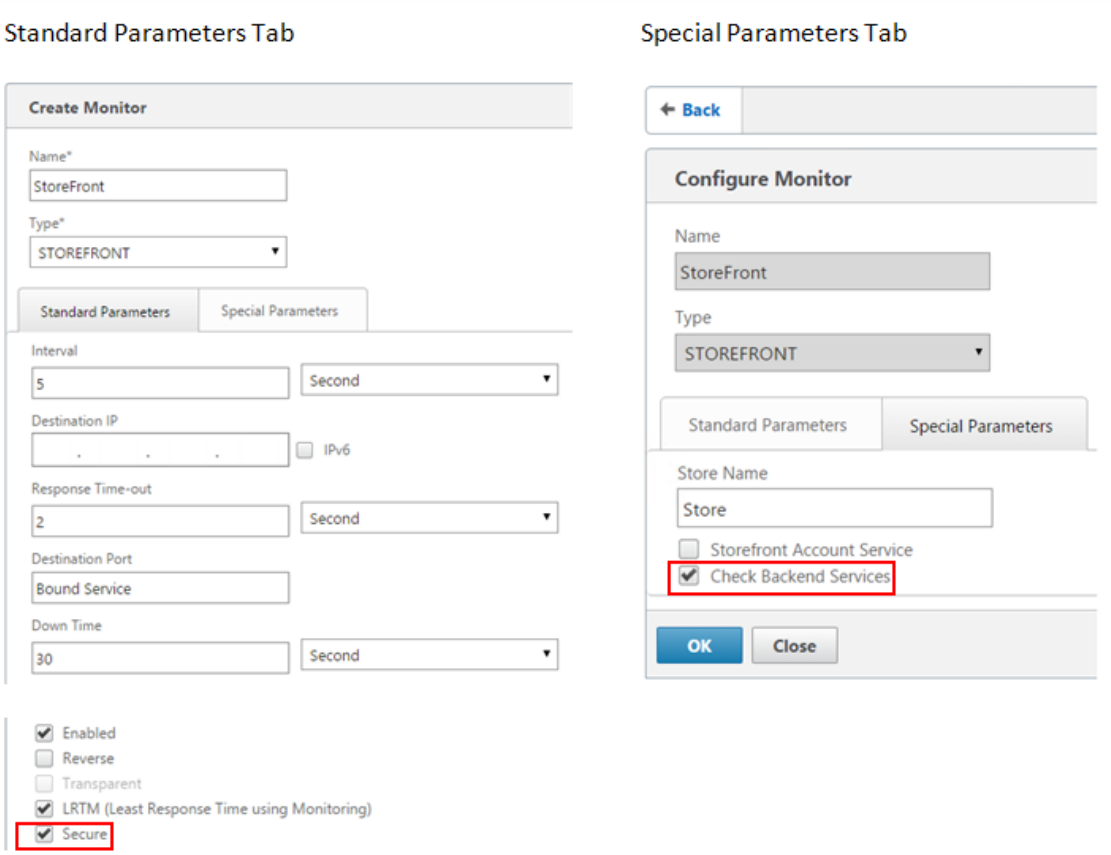
1. サービスグループ内で、右側のメンバーオプションを選択し、サーバーセクションで以前定義したすべてのStoreFrontサーバーノードを追加します。
2. HTTPポートを80に設定し、各サーバーに一意のサーバーIDを追加します。
3. ［Monitors］タブで前に作成したStoreFrontモニターを選択します。

ユーザートラフィック用SSL終了負荷分散仮想サーバーの作成

1. ［**Traffic Management**］>［**負荷分散**］>［**仮想サーバー**］>［**追加**］の順に選択し、新しい仮想サーバーを作成します。
2. 仮想サーバーが使用する負荷分散方式を選択します。StoreFront負荷分散で共通の選択は、［**round robin**］または［**least connection**］です。
3. 前に作成した**Service Group**を負荷分散仮想サーバーにバインドします。
4. 以前にサービスグループにバインドしたのと同じSSLおよびCA証明書を負荷分散仮想サーバーにバインドします。

   注：クライアントがHTTP Cookieを保存できない場合は、以降の要求にHTTP Cookieが含まれなくなり、**パーシステンス**は適用されません。

5. 負荷分散仮想サーバーメニュー内から［**Persistence**］を選択して、パーシステンス方式が**CookieInsert**となるように設定します。
6. cookieに名前を付けます。たとえば、デバッグ時にFiddlerトレースで見つけやすいように**NSC_SFPersistence**という名前を付けます。
7. バックアップパーシステンスを［**None**］に設定します。



サーバーグループ間のサブスクリプション同期用負荷分散仮想サーバーの作成

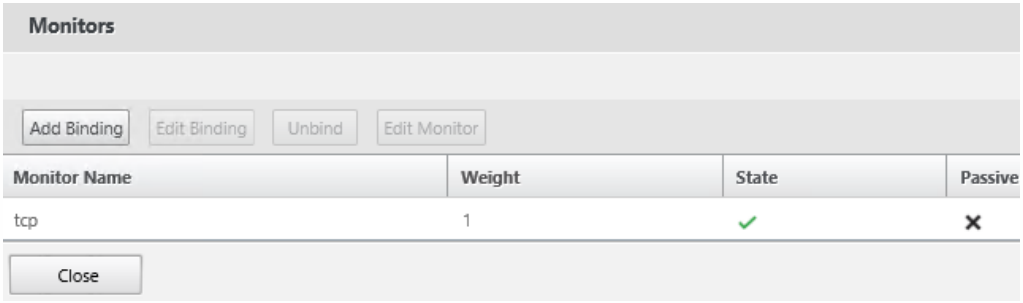
負荷分散仮想サーバーを作成する前に、次の点について検討します。

- **オプション1**：単一の仮想サーバーの作成：ユーザートラフィックのみを負荷分散。公開アプリケーションおよびデスクトップのICA起動のみを実行する場合は、必要なのはこれですべてです（必須、かつ通常はこれが必要なすべてです）。
- **オプション2**：仮想サーバーペアの作成：公開アプリケーションおよびデスクトップのICA起動を実行するためのユーザートラフィックの負荷分散用に1つ、サブスクリプションデータ同期操作の負荷分散用にもう1つ（大規模マルチサイト展開環境の2つ以上の負荷分散されたStoreFrontサーバーグループ間でサブスクリプションデータを反映させる場合にのみ必要）。

地理的に別々の場所にある2つ以上のStoreFrontサーバーグループで構成されるマルチサイト展開環境の場合、定期的にプル戦略を使ってサブスクリプションデータを複製できます。StoreFrontサブスクリプションレプリケーションはTCPポート808を使用するため、既存の負荷分散仮想サーバーをHTTPポート80またはSSL 443で使用することはできません。このサービスに対して高い可用性を提供するには、展開内の各NetScalerで2つ目の仮想サーバーを作成して、各StoreFrontサーバーグループのTCPポート808へ負荷分散します。レプリケーションスケジュールを構成する場合、サブスクリプション同期仮想サーバーの仮想IPアドレスと一致するサーバーグループアドレスを指定します。サーバーグループアドレスは、その場所にあるサーバーグループのロードバランサーのFQDNである必要があります。

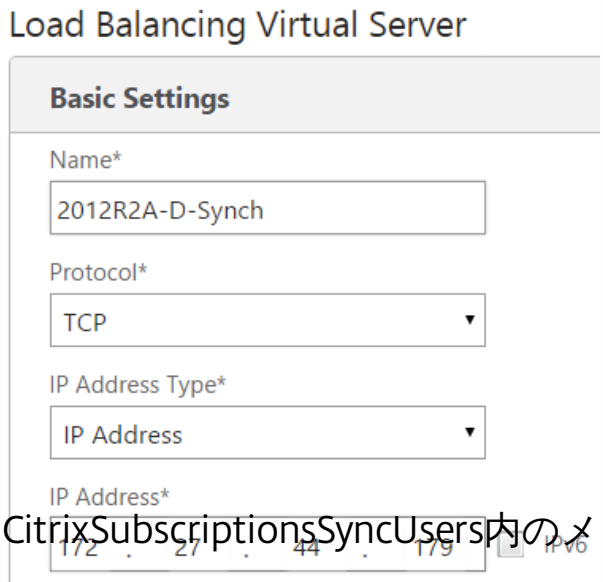
サブスクリプション同期用のサービスグループの構成

1. NetScaler管理GUIにログオンします。
2. **[Traffic Management] > [Service Groups] > [Add]** の順に選択し、新しいサービスグループを追加します。
3. プロトコルを **[TCP]** に変更します。
4. サービスグループ内で、右側の **[Members]** オプションを選択し、サーバーセクションで以前定義したすべてのStoreFrontサーバーノードを追加します。
5. **[Monitors]** タブで、TCPモニターを選択します。



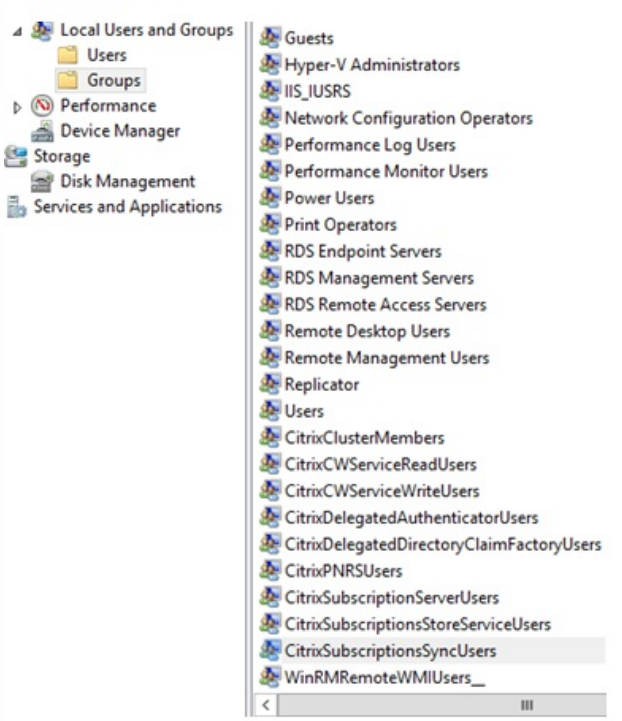
サーバーグループ間のサブスクリプション同期用負荷分散仮想サーバーの作成

1. NetScaler管理GUIにログオンします。
2. **[Traffic Management] > [Service Groups] > [Add]** の順に選択し、新しいサービスグループを追加します。
3. 負荷分散の手法に **[round robin]** を設定します。
4. プロトコルを **[TCP]** に変更します。
5. ポート番号には**443**ではなく、「**808**」と入力します。



CitrixSubscriptionsSyncUsers内のメンバーシップ

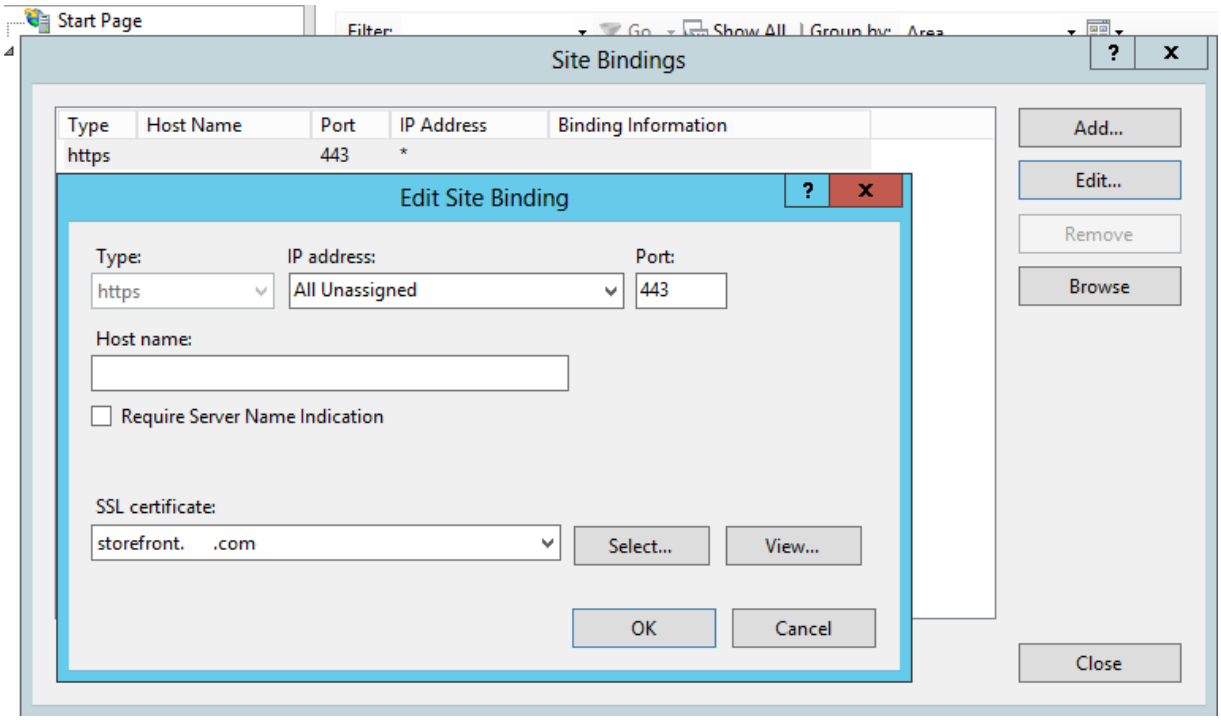
For **StoreFront server A** at **Location A** to request and pull subscription data from **server B** at a different location, server A must be a member of the **CitrixSubscriptionsSyncUsers** local security group on server B. The **CitrixSubscriptionsSyncUsers** local group contains an access control list of all remote StoreFront servers authorized to pull subscription data from a particular server. 双方向サブスクリプション同期の場合、サブスクリプションデータをプルするため、サーバーBもサーバーAの**CitrixSubscriptionsSyncUsers** セキュリティグループのメンバーである必要があります。



負荷分散用StoreFrontサーバーグループの構成

1. NetScaler負荷分散仮想サーバー上に展開されたのと同じ証明書と秘密キーをサーバーグループ内のすべてのStoreFrontノードにインポートします。

2. すべてのStoreFrontノードのIISにHTTPSバインドを作成し、そこにこれより前にインポートした証明書をバインドします。



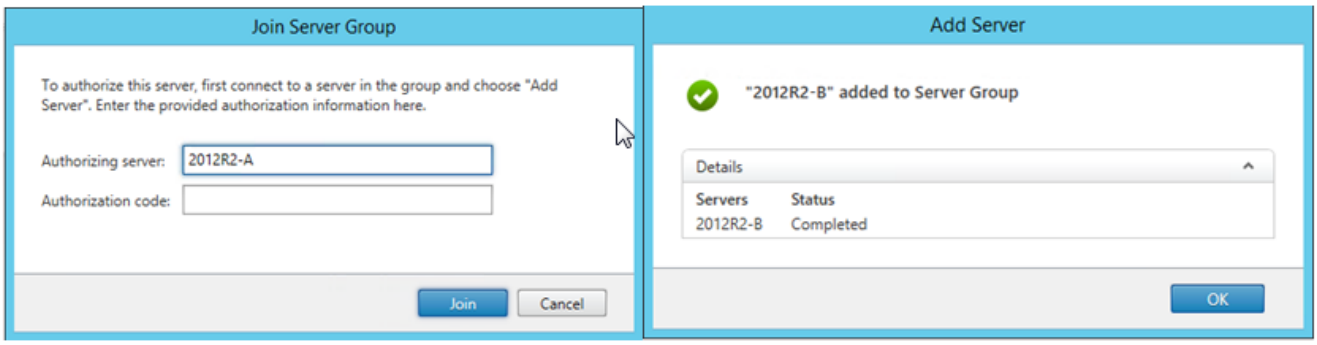
3. サーバーグループのすべてのノードにStoreFrontをインストールします。

4. StoreFrontをインストール間に、プライマリノードのホストベースURLがサーバーグループのすべてのメンバーによって使用される共有FQDNとなるように設定します。共通名（CN）またはサブジェクトの別名（SAN）として負荷分散されたFQDNを含む証明書を使用する必要があります。

「NetScaler負荷分散およびStoreFrontサーバーに対するSSL証明書の作成」を参照してください。

5. 初期StoreFront構成が完了したら、各ノードを順番にプライマリノードを使用するサーバーグループに参加させます。

6. 参加サーバーに対して **[サーバーグループ] > [サーバーの追加] > [Copy the Authorization Code]** の順に選択します。



7. プライマリノードからグループ内のすべてのほかのサーバーグループノードに構成を反映させます。

8. ロードバランサーの共有FQDNにアクセスして解決できるクライアントを使って、負荷分散サーバーグループをテストします。

Citrixサービスモニター

StoreFrontが依存しているWindowsサービスが適切に稼働しているかを確認する実行状態の外部監視を有効にするには、**Citrixサービスモニター**Windowsサービスを使用します。このサービスはほかのサービスには依存せず、ほかの重要なStoreFrontサービスの障害を監視して報告できます。モニターにより、StoreFrontサーバー展開の相対的な稼働状態をNetScalerなどほかのCitrixコンポーネントによって外部的に判断することができます。サードパーティソフトウェアは、StoreFrontモニターのXML応答を使用して、必要なStoreFrontサービスの状態を監視できます。

StoreFrontの展開後、HTTPおよびポート8000を使用するデフォルトのモニターが作成されます。

注：StoreFront展開内に存在できるのは、モニターの単一のインスタンスのみです。

プロトコルとポートをHTTPS 443に変更など、既存のデフォルトのモニターに対して何らかの変更を加えるには、3つのPowerShellコマンドレットを使ってStoreFrontモニターサービスURLを表示して再構成します。

デフォルトのサービスモニターを削除し、HTTPSおよびポート443を使用するものに置き換える

1. プライマリStoreFrontサーバーでPowerShell Integrated Scripting Environment（ISE）を開き、以下のコマンドを実行してデフォルトモニターをHTTPS 443に変更します。

次のように入力します。「Set-DSDerviceMonitorFeature –ServiceUrlhttps://localhost:443/StorefrontMonitor」

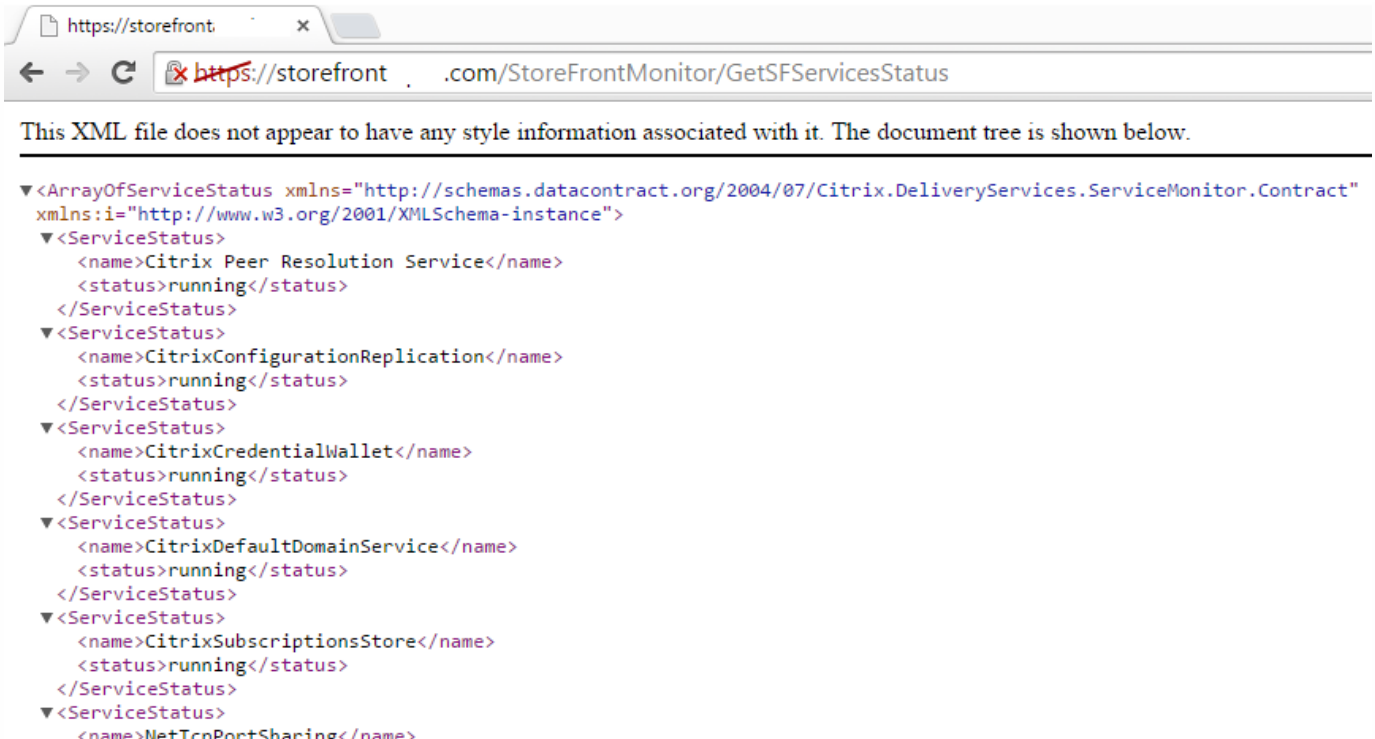
Set-STFServiceMonitor -ServiceUrl $ServiceUrl

Get-STFServiceMonitor

2. 変更が完了したら、StoreFrontサーバーグループ内の外のすべてのサーバーに変更を反映させます。

3. 新しいモニターでクイックテストを実行するには、StoreFrontサーバー、またはStoreFrontサーバーへネットワークアクセスするほかの任意のマシンでブラウザーに次のURLを入力します。ブラウザーは、すべてのStoreFrontサービスの状態についてXMLサマリーを返します。

https://:443/StoreFrontMonitor/GetSFServicesStatus

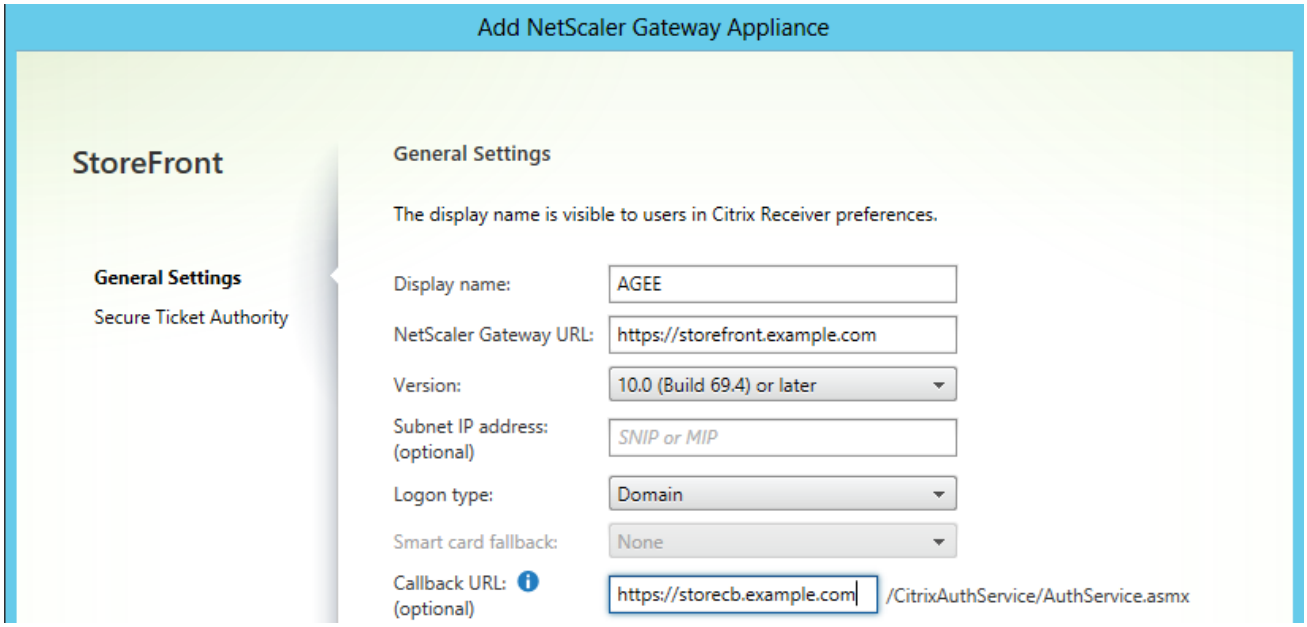


同じNetScaler Gatewayアプライアンス上のNetScaler Gatewayおよび負荷分散仮想サーバー

同じNetScalerアプライアンス上に構成済みのNetScaler Gateway仮想サーバーと負荷分散仮想サーバーがある場合、内部ドメインユーザーがNetScaler Gateway仮想サーバーを経由するのではなくStoreFront負荷分散ホストベースURLに直接アクセスしようとすると問題が発生することがあります。

この場合、StoreFrontはユーザーのソースIPアドレスとNetScaler GatewayのサブネットIPアドレス（SNIP）とを相関するものとするため、エンドユーザーがNetScaler Gatewayで既に認証されたとStoreFrontにより見なされてしまいます。このためStoreFrontは、ユーザーにドメイン資格情報を使ってログオンするよう求めるのではなく、AGBasicプロトコルを使ってNetScaler Gatewayサイレント認証を実行しようとします。この問題を避けるには、次に示すようにSNIPアドレスを省いてAGBasicでなく、ユーザー名とパスワードの認証が使用されるようにします。

StoreFrontサーバーグループでのNetscaler Gatewayの構成



NetScalerを使ってStoreFrontサーバーグループを負荷分散する場合のループバックオプション

2.6以前など古いバージョンのStoreFrontでは、各StoreFrontサーバーでホストファイルを手動で変更してロードバランサーの完全修飾ドメイン名（FQDN）を特定のStoreFrontサーバーのループバックアドレスまたはIPアドレスにマップするよう推奨していました。これにより、Receiver for Webは常に、負荷分散化された展開内の同じサーバー上のStoreFrontサービスと通信できます。これが必要なのは、Receiver for Webと認証サービス間の明示的なログインプロセス中にHTTPセッションが作成され、Receiver for WebがベースFQDNを使用してStoreFrontサービスと通信するためです。ベースFQDNがロードバランサーに対して解決された場合は、ロードバランサーは潜在的にグループ内の別のStoreFrontサーバーにトラフィックを送信でき、認証エラーが発生することになります。これによって、Receiver for Webはそれと同じサーバー上にあるストアサービスへアクセスしようとする場合を除き、ロードバランサーをバイパスしません。

PowerShellを使ってループバックオプションを設定できます。ループバックを有効にすると、サーバーグループ内の各StoreFrontサーバーにホストファイルエントリを作成する必要がなくなります。

Receiver for Web web.configファイルの例：

PowerShellコマンドの例：

& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.ps1"

Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "OnUsingHttp" -LoopbackPortUsingHttp 81

-Loopback パラメーターには3つの値を設定できます。

値	コンテキスト
On： URLのホストを127.0.0.1に変更します。スキーマおよびポート（指定されている場合）は変更されません。	SSL終了ロードバランサーが使用されている場合は使用できません。
OnUsingHttp： ホストを127.0.0.1に、スキーマをHTTPに変更し、ポートを**loopbackPortUsingHttp**属性に構成されている値に変更します。	ロードバランサーがSSL終了である場合のみ使用します。ロードバランサーとStoreFrontサーバー間の通信はHTTPで行います。-loopbackPortUsingHttp属性を使って、HTTPポートを明示的に構成できます。
Off： 要求内のURLはいかなる方法によっても変更されません。	トラブルシューティングに使用します。Fiddlerのようなツールは、ループバックを“On”に設定している場合、Citrix Receiver for WebとStoreFront Services間のトラフィックをキャプチャできません。

Configure two URLs for the same NetScaler Gateway

May 22, 2017

In StoreFront, you can add a single NetScaler Gateway URL from the StoreFront management console in Manage NetScaler Gateways > Add or Edit. It is also possible to add both a public NetScaler Gateway URL and a GSLB (Global Server Load Balancing) URL in Manage NetScaler Gateways > imported from file.

This article shows you how to use PowerShell cmdlets and the StoreFront PowerShell SDK to use an optional parameter, -gslburl, to set the GslbLocation attribute of a gateway. This feature simplifies the NetScaler Gateway administration in StoreFront in the following use cases:

1. **GSLB and multiple NetScaler Gateways**. Use GSLB and multiple NetScaler Gateways to load balance remote connections to published resources in two or more locations within a large global Citrix deployment.
2. **Single NetScaler Gateway using a public or private URL**. Use the same NetScaler Gateway for external access using a public URL, and for internal access using a private URL.

This is an advanced feature. If you are new to GSLB concepts, see the Related information links at the end of this article.

This feature offers the following benefits:

- Support two simultaneous URLs for a single gateway object.
- Users can switch between two different URLs to access the NetScaler Gateway without the administrator reconfiguring the StoreFront gateway object to match the gateway URL the user wants to use.
- Shorter setup and test times to validate the StoreFront gateway configuration when using multiple GSLB gateways.
- Use the same NetScaler Gateway object in StoreFront inside the DMZ for both external and internal access.
- Support both URLs for optimal gateway routing. For more information on optimal gateway routing, see Set up highly available multi-site stores.

Deployment considerations when using two Gateway URLs

> ### Important
>
> Before configuring a second gateway URL using the -gslburl parameter, Citrix recommends reviewing what server certificates you have in place and how your organization performs DNS resolution. Any URLs that you want to use in your NetScaler and StoreFront deployment must be present in your server certificates. For more information about server certificates, see Plan gateway and server certificate usage.

DNS

- **Split DNS**. It is common for large enterprises to use split DNS. Split DNS involves using different namespaces and different DNS servers for public and private DNS resolution. Check if you have the existing DNS infrastructure to support this.
- **Single URL for external and internal access to published resources**. Decide if you want to use the same URL to access published resources from both outside and inside your corporate network, or consider if two different URLs are acceptable such as example.com and example.net.

Server certificate examples

This section contains example server certificate deployments when using two Gateway URLs.

- **Example server certificate for a load balanced StoreFront deployment**

  A privately signed wildcard server certificate should contain the FQDN *.storefront.example.net.

  Or

  A privately signed SAN server certificate should contain all the FQDNs needed to load balance three StoreFront servers.

  loadbalancer.storefront.example.net

  server1.storefront.example.net

  server2.storefront.example.net

  server3.storefront.example.net

  Set the host base URL of the Storefront server group to be the shared FQDN, which resolves to the load balancer IP address.

  loadbalancer.storefront.example.net

- **Example server certificate for a group of XenApp and XenDesktop 7.x Delivery Controllers**

  A privately signed wildcard server certificate should contain the FQDN *.xendesktop.example.net.

  Or

  A privately signed SAN server certificate should contain all the server FQDNs needed for a XenDesktop site containing four Controllers.

  XD1A. xendesktop.example.net

  XD1B. xendesktop.example.net

  XD2A. xendesktop.example.net

  XD2B. xendesktop.example.net

- **Example server certificate for a NetScaler Gateway which is accessed both externally and internally using split DNS**

  A publically signed SAN server certificate for both external and internal access should contain both the external and internal FQDNs.

  gateway.example.com

  gateway.example.net

- **Example server certificate for all GSLB Gateways which are accessed externally**

  A publically signed SAN server certificate for external access through GSLB should contain the FQDNs.

gslbdomain.example.com

emeagateway.example.com

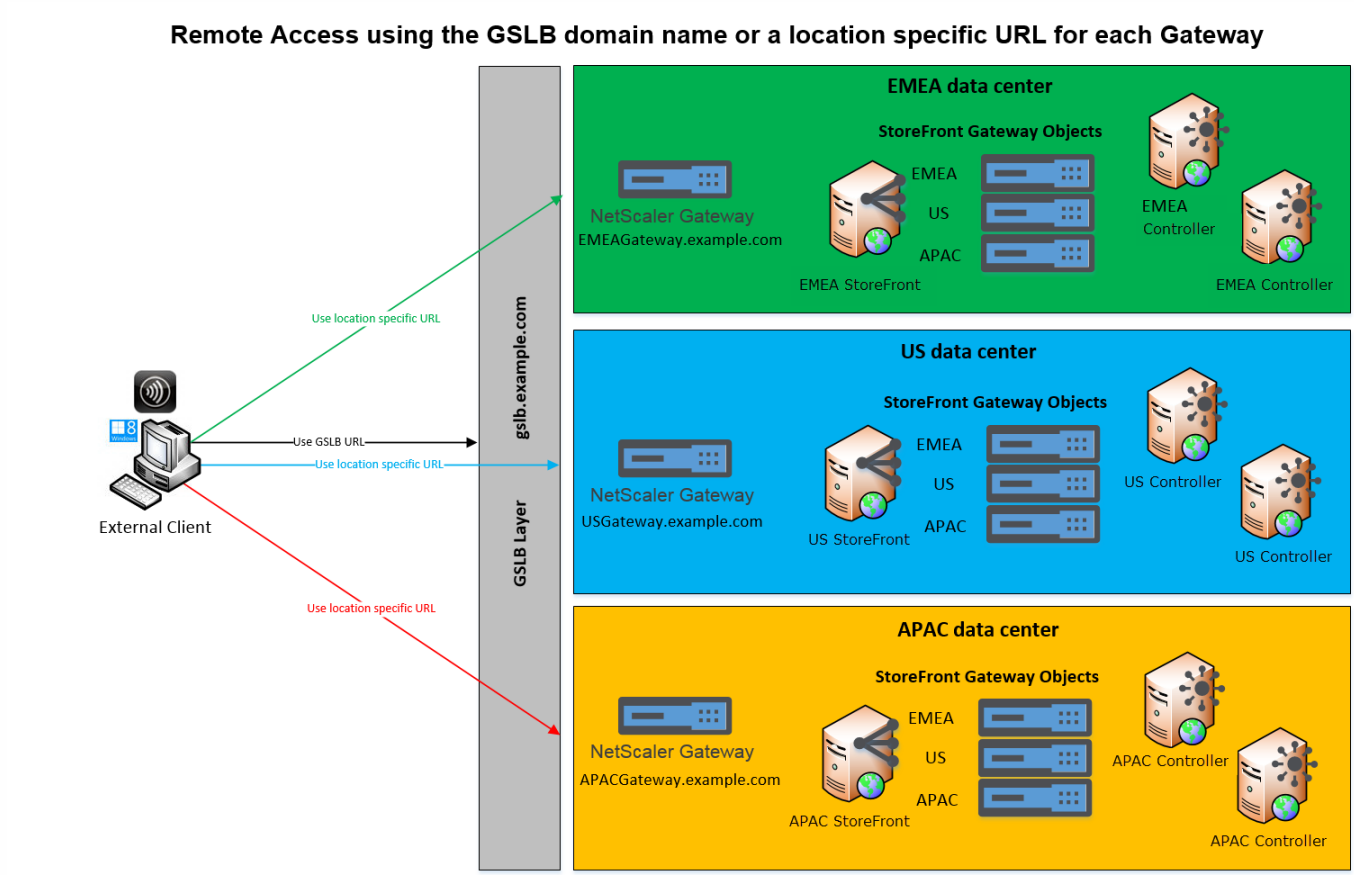
usgateway.example.com

apacgateway.example.com

This allows the user to access the closest gateway using GSLB or to pick a gateway in the location of their choice using its unique FQDN.

Use Case #1: GSLB and multiple NetScaler Gateways

The administrator uses GSLB and multiple NetScaler Gateways to load balance remote connections to published resources in two or more locations within a large global Citrix deployment.



In this example:

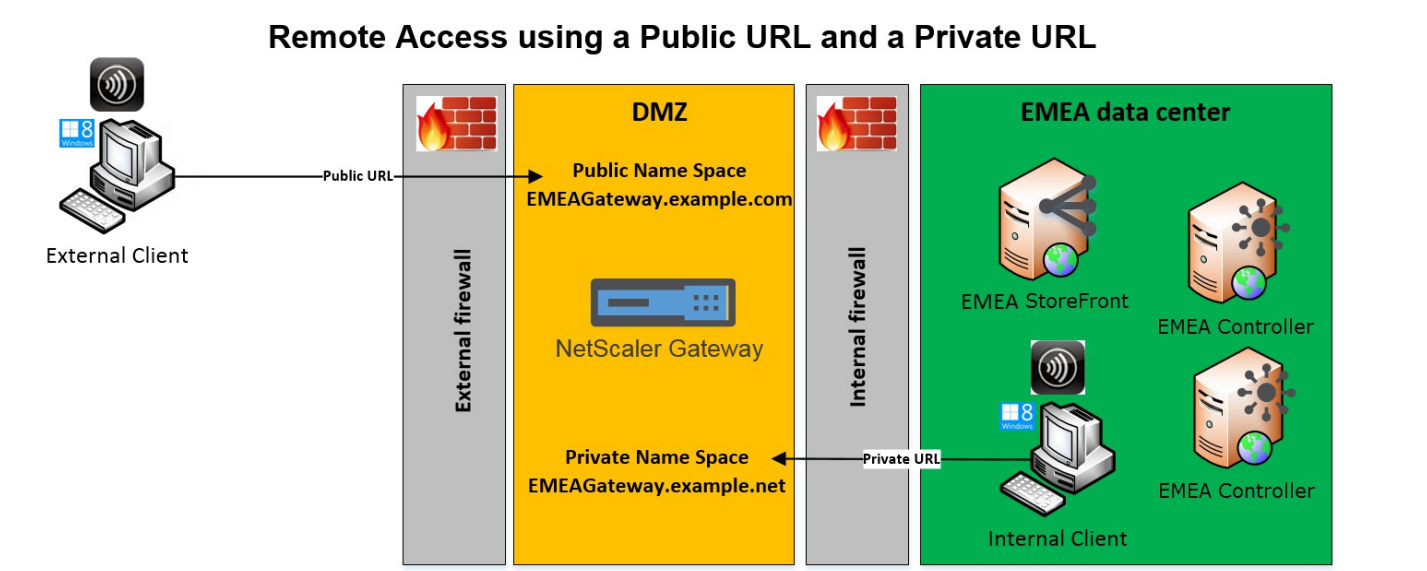
- Each location or data center contains at least one gateway, one or more StoreFront servers, and one or more XenApp and XenDesktop Controllers to provide published resources for that location.
- Each GSLB service configured on the GSLB NetScalers within the global deployment represents a gateway VPN vServer. All of the StoreFront servers in the deployment must be configured to contain all of the NetScaler Gateway vServers that make up the GSLB layer.
- The GSLB NetScaler Gateways are used in active/active mode but can also provide failover if the network connection, DNS, gateway, StoreFront server or XenApp and XenDesktop Controllers at one location fail. Users are automatically

directed to another gateway if a GSLB service is unavailable.

- External clients are directed to the closest gateway based on the configured GSLB load balancing algorithm such as round trip time (RTT) or Static Proximity when making remote connections.
- The unique URL for each gateway allows users to manually select which data center they want to launch resources from by choosing the location-specific URL for the gateway they want to use.
- GSLB can be bypassed when GSLB or a DNS delegation is not working as expected. Users can continue to access remote resources at any data center using its location-specific URL until any GSLB related issues are resolved.

Use Case #2: Single NetScaler Gateway using a public or private URL

The administrator uses the same NetScaler Gateway for both external access using a public URL, and also internally using a private URL.



In this example:

- The administrator wants all access to published resources and HDX launch traffic to pass through a NetScaler Gateway even if the client is internal.
- The NetScaler is located in a DMZ.
- There are two different network routes to the NetScaler Gateway through the two firewalls on either side of the DMZ.
- The public-facing, external namespace is different from the internal namespace.

PowerShell cmdlet examples

Use the PowerShell cmdlets **Add-STFRoamingGateway** and **Set-STFRoamingGateway** with the parameter, -gslburl, to set the **GslbLocation** attribute on the StoreFront gateway object. For example:

```
command
```

コピー

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.cor

Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com

Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA gateway object)

Or

Get-STFRoamingGateway (returns all gateway object configured in StoreFront)
```

For use case #1, the following gateways are returned using **Get-STFRoamingGateway**:

command コピー

Name: **EMEAGateway**

Location: **https://emeagateway.example.com/** (Unique URL for the EMEA Gateway)

GslbLocation: **https://gslb.example.com/** (GSLB URL for all three gateways)

Name: **USGateway**

Location: **https://USgateway.example.com/** (Unique URL for the US Gateway)

GslbLocation: **https://gslb.example.com/** (GSLB URL for all three gateways)

Name: **APACGateway**

Location: **https://APACgateway.example.com/** (Unique URL for the APAC Gateway)

GslbLocation: **https://gslb.example.com/** (GSLB URL for all three gateways)

For use case #2: the following gateways are returned using **Get-STFRoamingGateway**:

command コピー

Name: **EMEAGateway**

Location: **https://emeagateway.example.com/** (Public URL for the Gateway)

GslbLocation: **https://emeagateway.example.net/** (Private URL for the Gateway)

For use case #1, Optimal Gateway Routing is returned using **Get-STFStoreRegisteredOptimalLaunchGateway**:

command コピー

```
$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}**

GSLB URL or Internal URL for each Gateway is stored in the Roaming service web.config file

StoreFront does not display the GSLB URL or internal URL for each Gateway within the StoreFront management console, however it is possible to view the configured GSLBLocation path for all GSLB gateways by opening the roaming service Web.Config file location in C:\inetpub\wwwroot\Citrix\Roaming\web.config on the StoreFront server.

Use Case #1 Gateways in Roaming web.config file

```
<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>
```

Use Case #2: Gateways in Roaming web.config file

```
<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>
```

Configure NetScaler and StoreFront for Delegated Forms Authentication (DFA)

May 22, 2017

Extensible authentication provides a single customization point for extension of NetScaler's and StoreFront's form-based authentication. To achieve an authentication solution using the Extensible Authentication SDK, you must configure Delegated Form Authentication (DFA) between NetScaler and StoreFront. The Delegated Forms Authentication protocol allows generation and processing of authentication forms, including credential validation, to be delegated to another component. For example, NetScaler delegates it authentication to StoreFront, which then interacts with a third party authentication server or service.

Installation recommendations

- To ensure communication between NetScaler and StoreFront is protected, use HTTPS instead of HTTP protocol.
- For cluster deployment, ensure that all the nodes have the same server certificate installed and configured in IIS HTTPS binding prior to configuration steps.
- Ensure that Netscaler has the issuer of StoreFront's server certificate as a trusted certificate authority when HTTPS is configured in StoreFront.

StoreFront cluster installation considerations

- Install a third party authentication plugin on all the nodes prior to joining them up together.
- Configure all the Delegated Forms Authentication related settings on one node and propagate the changes to the others. See the "Enable Delegated Forms Authentication."

Enable Delegated Forms Authentication

Because there is no GUI to setup Citrix pre-shared key setting in StoreFront, use the PowerShell console to install Delegated Forms Authentication.

1. Install Delegated Forms Authentication. It is not installed by default and you need to install it using the PowerShell console.

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\ImportModules.ps1
Adding snapins
Importing modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-DSDFAServer
Id                        : bf694fbc-ae0a-4d56-8749-c945559e897a
ClassType                 : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc
FrameworkController       : Citrix.DeliveryServices.Framework.FileBased.FrameworkController
ParentInstance            : 8dd182c7-f970-466c-ad4c-27a5980f716c
RootInstance              : 5d0cdc75-1dee-4df7-8069-7375d79634b3
TenantId                  : 860e9401-39c8-4f2c-928d-34251102b840
Data                      : {}
ReadOnlyData              : {[Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer
                            vices.Web.Commands], [Tenant, 860e9401-39c8-4f2c-928d-34251102b840]}
ParameterData             : {[FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f
                            970-466c-ad4c-27a5980f716c], [TenantId, 860e9401-39c8-4f2c-928d-34251102b840]}
AdditionalInstanceDependencies : {b1e48ef0-b9e5-4697-af9b-0910062aa2a3}
IsDeployed                : True
FeatureClass              : Citrix.DeliveryServices.Framework.Feature.FeatureClass
```

2. Add Citrix Trusted Client. Configure the shared secret key (passphrase) between StoreFront and Netscaler. Your passphrase and client ID must be identical to what you configured in NetScaler.
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
3. Set the Delegated Forms Authentication conversation factory to route all the traffic to the custom form. To find the conversation factory, look for ConversationFactory in C:\inetpub\wwwroot\Citrix\Authentication\web.config.This is an example of what you might see.

```
<example connectorURL="http://Example.connector.url:8080/adapters-sf-aaconnector-webapp">
    <routeTable order="1000">
     <routes>
      <route name="StartExampleAuthentication" url="Example-Bridge-Forms/Start">
       <defaults>
        <add param="controller" value="ExplicitFormsAuthentication" />
        <add param="action" value="AuthenticateStart" />
        <add param="postbackAction" value="Authenticate" />
        <add param="cancelAction" value="CancelAuthenticate" />
        <add param="conversationFactory" value="ExampleBridgeAuthentication" />
        <add param="changePasswordAction" value="StartChangePassword" />
        <add param="changePasswordController" value="ChangePassword" />
        <add param="protocol" value="CustomForms" />
       </defaults>
      </route>
```

4. In PowerShell, set the Delegated Forms Authentication conversation factory. In this example, to ExampleBridgeAuthentication.
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication

PowerShell arguments are not case-sensitive: -ConversationFactory is identical to -conversationfactory.

Uninstall StoreFront

Before you uninstall StoreFront, uninstall any third party authentication plugin, as it will impact the functionality of StoreFront.

ビーコンポイントの構成

May 22, 2017

ビーコンポイントとして使用する、内部ネットワークの内側と外側のURLを指定するには、[ビーコンの管理] タスクを使用します。Citrix Receiverは、ユーザーがローカルネットワークと公共のネットワークのどちらに接続しているのかをビーコンポイントを使用して識別します。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーがそのユーザーの位置情報に基づいて適切な接続詳細をCitrix Receiverに返します。これにより、ユーザーがデスクトップやアプリケーションにアクセスするときに再ログオンする必要がなくなります。

たとえば、内部ビーコンポイントにアクセス可能な場合、そのユーザーはローカルネットワークに接続していると認識されます。これに対し、Citrix Receiverで内部ビーコンポイントにアクセスできず、2つの外部ビーコンポイントからの応答を受信した場合、そのユーザーは社内ネットワークの外からインターネット経由で接続していると認識されます。この場合、このユーザーはデスクトップやアプリケーションにNetScaler Gateway経由で接続する必要があります。ユーザーがデスクトップやアプリケーションにアクセスすると、そのリソースを提供するサーバーが、使用されるべきNetScaler Gatewayアプライアンスの詳細を提供します。このため、ユーザーがそのNetScaler Gatewayアプライアンスにログオンする必要はありません。

StoreFrontでは、内部ビーコンポイントとしてデフォルトでサーバーのURLまたは負荷分散URLが使用されます。外部ビーコンポイントは、デフォルトでCitrix社のWebサイト、および管理者が追加した最初のNetScaler Gateway仮想サーバーまたはユーザーログオンポイント（Access Gateway 5.0の場合）のURLが使用されます。

ビーコンポイントの設定を変更する場合は、そのビーコンポイントをユーザーに通知してCitrix Receiverの設定を変更させる必要があります。ストアのReceiver for Webサイトが構成済みの場合、ユーザーはそのサイトから最新のCitrix Receiverプロビジョニングファイルを入手できます。Citrix Receiver for Webサイトが構成済みでない場合は、管理者がストアのプロビジョニングファイルをエクスポートしてユーザーに提供します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. Windowsの［スタート］画面または［アプリ］画面で、［Citrix StoreFront］タイルをクリックします。
2. Citrix StoreFront管理コンソールの左ペインで **[ストア]** ノードを選択して、［操作］ペインの［ビーコンの管理］をクリックします。
3. 内部ビーコンポイントとして使用するURLを指定します。
   - StoreFront展開環境でサーバーのURLまたは負荷分散URLを使用するには、［サービスURLを使用する］を選択します。
   - 別のURLを使用するには、［ビーコンアドレスを指定する］を選択して、内部ネットワーク内の可用性の高いURLを入力します。
4. 外部ビーコンポイントのURLを入力するには、［追加］をクリックします。ビーコンポイントを変更するには、［外部ビーコン］ボックスの一覧でURLを選択して［編集］をクリックします。ビーコンポイントとしてそのアドレスが使われないようにするには、一覧でURLを選択して［削除］をクリックします。
   公共のネットワーク上で解決でき、可用性の高い外部ビーコンポイントを少なくとも2つ指定する必要があります。ビーコンURLは、http://domainなどの簡略化されたNetBIOS名ではなく、http://domain.comなどの完全修飾ドメイン名にする必要があります。これにより、内部ネットワークとユーザーの間に、ホテルやインターネットカフェなど、インターネットペイウォール（有料の壁）があるかどうかをCitrix Receiverで判別できるようになります。インターネットペイウォールがある場合、すべての外部ビーコンポイントが同じプロキシに接続されます。

詳細構成

May 22, 2017

StoreFrontコンソールにより、PowerShell、証明書プロパティ、または構成ファイルを使って構成できる詳細オプションを有効にできます。

デスクトップアプライアンスサイトの構成	デスクトップアプライアンスサイトを作成、削除、および変更します。
ストアに内部および外部アクセスするための単一のFQDNの作成	会社のネットワーク内外のクライアント用に単一の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を作成することで、そのネットワーク内、およびネットワーク外からNetScaler Gateway経由でリソースにアクセスするユーザーの使い勝手を簡素化します。
リソースフィルターの構成	リソースの種類やキーワードを使用して、列挙されるリソースを指定します。

Configure Desktop Appliance sites

May 22, 2017

The tasks below describe how to create, remove, and modify Desktop Appliance sites. To create or remove sites, you execute Windows PowerShell commands. Changes to Desktop Appliance site settings are made by editing the site configuration files.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

Note: The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

To create or remove Desktop Appliance sites

Only a single store can be accessed through each Desktop Appliance site. You can create a store containing all the resources you want to make available to users with non-domain-joined desktop appliances. Alternatively, create separate stores, each with a Desktop Appliance site, and configure your users' desktop appliances to connect to the appropriate site.

1. Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, type the following command to import the StoreFront modules.
   & "installationlocation\Scripts\ImportModules.ps1"
   Where installationlocation is the directory in which StoreFront is installed, typically C:\Program Files\Citrix\Receiver StoreFront\.

2. To create a new Desktop Appliance site, type the following command.
   Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid
   -VirtualPath sitepath -UseHttps {$False | $True}
   -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}]
   [-EnableExplicit {$True | $False}] [-EnableSmartCard {$False | $True}]
   [-EnableEmbeddedSmartCardSSO {$False | $True}]
   Where sitename is a name that helps you to identify your Desktop Appliance site. For iisid, specify the numerical ID of the Microsoft Internet Information Services (IIS) site hosting StoreFront, which can be obtained from the Internet Information Services (IIS) Manager console. Replace sitepath with the relative path at which the site should be created in IIS, for example, /Citrix/DesktopAppliance. Note that Desktop Appliance site URLs are case sensitive.

   Indicate whether StoreFront is configured for HTTPS by setting -UseHttps to the appropriate value.

   To specify the absolute URL of the store service used by the Desktop Appliance Connector site, use StoreUrl storeaddress. This value is displayed for the Store summary in the administration console.

   By default, when a user logs on to a Desktop Appliance site, the first desktop available to the user starts automatically. To configure your new Desktop Appliance site to enable users to choose between multiple desktops, if available, set -EnableMultiDesktop to $True.

   Explicit authentication is enabled by default for new sites. You can disable explicit authentication by setting the -

EnableExplicit argument to $False. Enable smart card authentication by setting -EnableSmartCard to $True. To enable pass-through with smart card authentication, you must set both -EnableSmartCard and -EnableEmbeddedSmartCardSSO to $True. If you enable explicit and either smart card or pass-through with smart card authentication, users are initially prompted to log on with a smart card, but can fall back to explicit authentication if they experience any issues with their smart cards.

The optional arguments configure settings that can also be modified after the Desktop Appliance site has been created by editing the site configuration file.

Example:

Create a Desktop Appliance Connector site at virtual path /Citrix/DesktopAppliance1 in the default IIS web site.

```
Install-DSDesktopAppliance `

-FriendlyName DesktopAppliance1 `

-SiteId 1 `

-VirtualPath /Citrix/DesktopAppliance1 `

-UseHttps $false `

-StoreUrl https://serverName/Citrix/Store `

-EnableMultiDesktop $true `

-EnableExplicit $true `

-EnableSmartCard $true `

-EnableEmbeddedSmartCardSSO $false
```

3. To remove an existing Desktop Appliance site, type the following command.
   Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
   Where iisid is the numerical ID of the IIS site hosting StoreFront and sitepath is the relative path of the Desktop Appliance site in IIS, for example, /Citrix/DesktopAppliance.

4. To list the Desktop Appliance sites currently available from your StoreFront deployment, type the following command.
   Get-DSDesktopAppliancesSummary

To configure user authentication

Desktop Appliance sites support explicit, smart card, and pass-through with smart card authentication. Explicit authentication is enabled by default. If you enable explicit and either smart card or pass-through with smart card authentication, the default behavior initially prompts users to log on with a smart card. Users who experience issues with their smart cards are given the option of entering explicit credentials. If you configure IIS to require client certificates for HTTPS connections to all StoreFront URLs, users cannot fall back to explicit authentication if they cannot use their smart cards. To configure the authentication methods for a Desktop Appliance site, you edit the site configuration file.

1. Use a text editor to open the web.config file for the Desktop Appliance site, which is typically located in the C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance directory, where storename is the name specified for the store when it was created.

2. Locate the following element in the file.
   <explicitForms enabled="true" />
3. Change the value of the enabled attribute to false to disable explicit authentication for the site.
4. Locate the following element in the file.
   <certificate enabled="false" useEmbeddedSmartcardSso="false"
   embeddedSmartcardSsoPinTimeout="00:00:20" />
5. Set the value of the enabled attribute to true to enable smart card authentication. To enable pass-through with smart card authentication, you must also set the value of the useEmbeddedSmartcardSso attribute to true. Use the embeddedSmartcardSsoPinTimeout attribute to set the time in hours, minutes, and seconds for which the PIN entry screen is displayed before it times out. When the PIN entry screen times out, users are returned to the logon screen and must remove and reinsert their smart cards to access the PIN entry screen again. The time-out period is set to 20 seconds by default.

To enable users to choose between multiple desktops

By default, when a user logs on to a Desktop Appliance site, the first desktop (in alphabetical order) available to the user in the store for which the site is configured starts automatically. If you provide users with access to multiple desktops in a store, you can configure the Desktop Appliance site to display the available desktops so users can choose which one to access. To change these settings, you edit the site configuration file.

1. Use a text editor to open the web.config file for the Desktop Appliance site, which is typically located in the C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance directory, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.
   <resources showMultiDesktop="false" />
3. Change the value of the showMultiDesktop attribute to true to enable users to see and select from all the desktops available to them in the store when they log on to the Desktop Appliance site.

Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally

May 22, 2017

Note: To use this feature with native desktop receivers, the following versions are required.

- Windows Receiver 4.2
- MAC Receiver 11.9

You can provide access to resources from within your corporate network and from the Internet through a NetScaler Gateway and simplify the user experience by creating a single FQDN for both internal and roaming external clients.

Creating a single FQDN is helpful to users who configure any of the native Receivers. They need remember only a single URL whether they are currently connected to an internal or public network.

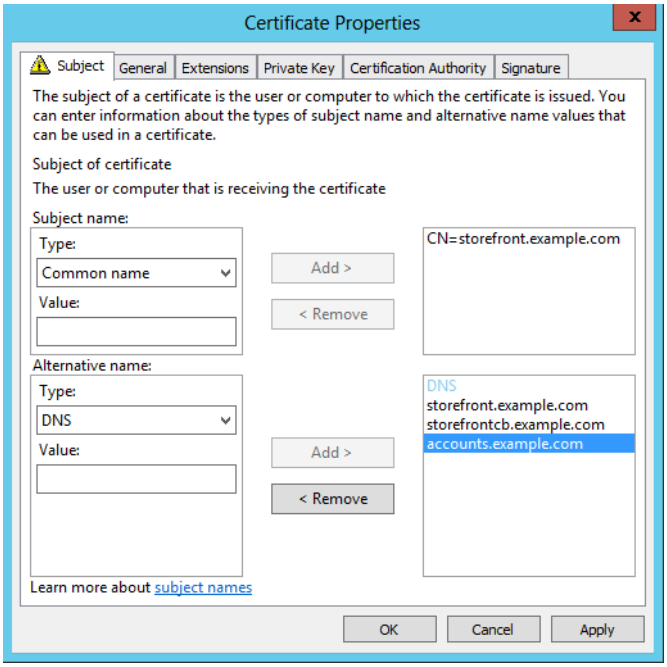
StoreFront beacons for native Receivers

Citrix Receiver attempts to contact beacon points and uses the responses to determine whether users are connected to local or public networks. When a user accesses a desktop or application, the location information is passed to the server providing the resource so that appropriate connection details can be returned to Citrix Receiver. This ensures that users are not prompted to log on again when they access a desktop or application. For information about configuring beacon points, see Configure beacon points.

Configure the NetScaler Gateway vServer and SSL Certificate

The shared FQDN resolves either to an external firewall router interface IP or NetScaler Gateway vServer IP in the DMZ when external clients try to access resources from outside of the corporate network. Ensure the Common Name and Subject Alternative Name fields of the SSL certificate contain the shared FQDN to be used to access the store externally. By using a third party root CA such as Verisign instead of an enterprise Certification Authority (CA) to sign the gateway certificate, any external client automatically trusts the certificate bound to the gateway vServer. If you use a third party root CA such as Verisign, no additional root CA certificates need to be imported on to external clients.

To deploy a single certificate with the Common Name of the shared FQDN to both the NetScaler Gateway and the StoreFront server, consider whether you want to support remote discovery. If so, make sure the certificate follows the specification for the Subject Alternative Names.



NetScaler Gateway vServer example certificate: storefront.example.com

1. Ensure that the shared FQDN, the callback URL, and the accounts alias URL are included in the DNS field as Subject Alternative Name (SANs).
2. Ensure that the private key is exportable so the certificate and key can be imported into the NetScaler Gateway.
3. Ensure that Default Authorization is set to Allow.
4. Sign the certificate using a third party CA such as Verisign or an enterprise root CA for your organization.

Two-node server group example SANs:

storefront.example.com (mandatory)

storefrontcb.example.com (mandatory)

accounts.example.com (mandatory)

storefrontserver1.example.com (optional)

storefrontserver2.example.com (optional)

Sign the Netscaler Gateway vServer SSL certificate using a Certification Authority (CA)

Based on your requirements, you have two options for choosing the type of CA signed certificate.

- Option 1 - Third Party CA signed certificate: If the certificate bound to the Netscaler Gateway vServer is signed by a trusted third party, external clients will likely NOT need any root CA certificates copied to the their trusted root CA certificate stores. Windows clients ship with the root CA certificates of the most common signing agencies. Examples of commercial third party CAs that could be used include DigiCert, Thawte, and Verisign. Note that mobile devices such as iPads, iPhones, and Android tablets and phones might still require the root CA to be copied onto the device to trust the NetScaler Gateway vServer.
- Option 2 - Enterprise Root CA signed certificate: If you choose this option, every external client requires the enterprise root CA certificate copied to their trusted root CA stores. If using portable devices with native Receiver installed, such as iPhones and iPads, create a security profile on these devices.

Import the root certificate into portable devices

- iOS devices can import .CER x.509 certificate files using email attachments, because accessing the local storage of iOS devices is usually not possible.
- Android devices require the same .CER x.509 format. The certificate can be imported from the device local storage or email attachments.

External DNS: storefront.example.com

Ensure that the DNS resolution provided by your organization's Internet service provider resolves to the externally facing IP of the firewall router on the outside edge of DMZ or to the NetScaler Gateway vServer VIP.

Split view DNS

- When split-view DNS is correctly configured, the source address of the DNS request should send the client to the correct DNS A record.
- When clients roam between public and corporate networks, their IP should change. Depending on the network to which they are currently connected, they should receive the correct A record when they query storefront.example.com.

Import certificates issued from a Windows CA to NetScaler Gateway

WinSCP is a useful and free third party tool to move files from a Windows machine to a NetScaler Gateway file system. Copy certificates for import to the /nsconfig/ssl/ folder within the NetScaler Gateway file system. You can use the OpenSSL tools on the NetScaler Gateway to extract the certificate and key from a PKCS12/PFX file to create two separate .CER and .KEY X.509 files in PEM format that can be used by the NetScaler Gateway

1. Copy the PFX file into /nsconfig/ssl on the NetScaler Gateway appliance or VPX.
2. Open the NetScaler Gateway command line interface.
3. To switch to the FreeBSD shell, type Shell to exit the NetScaler Gateway command line interface.
4. To change directory, use cd /nsconfig/ssl.
5. Run openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer and enter the PFX password when prompted.
6. Run openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key
7. Enter the PFX password when prompted and then set a private key PEM passphrase to protect the .KEY file.
8. To ensure that the .CER and .KEY files were successfully created inside /nsconfig/ssl/, run ls –al.
9. To return to the NetScaler Gateway command line interface, type Exit.

Native Windows/Mac Receiver Gateway session policy

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

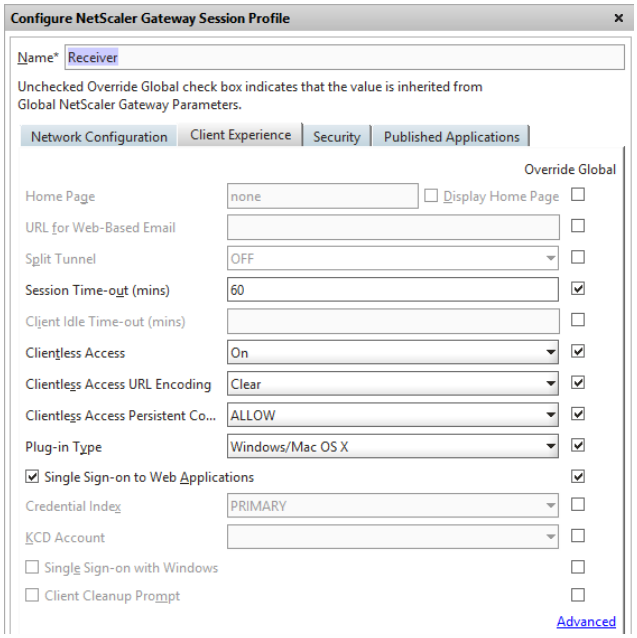
Receiver for Web Gateway session policy

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

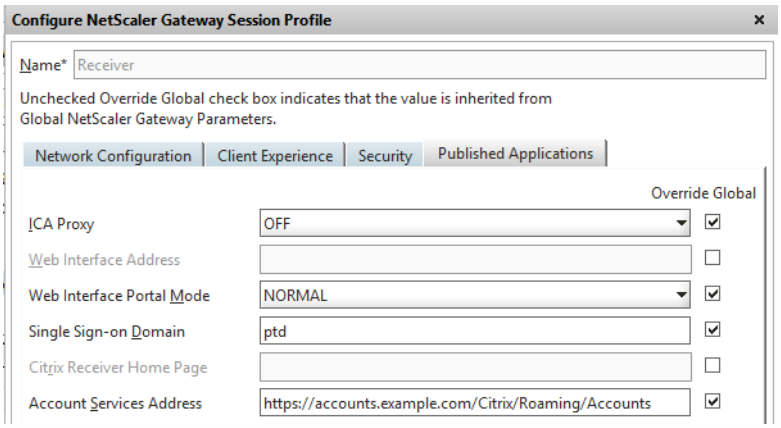
cVPN and Smart Access Settings

If you use SmartAccess, enable smart access mode on the NetScaler Gateway vServer properties page. Universal Licenses are required for every concurrent user who accesses remote resources.

Receiver profile

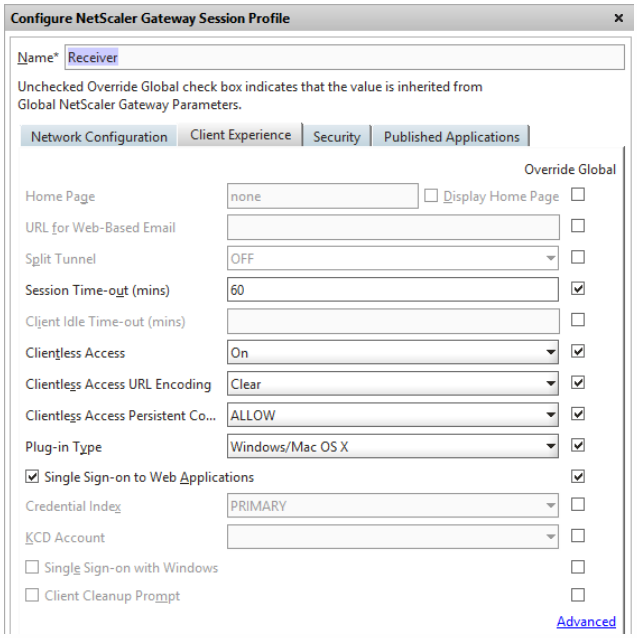


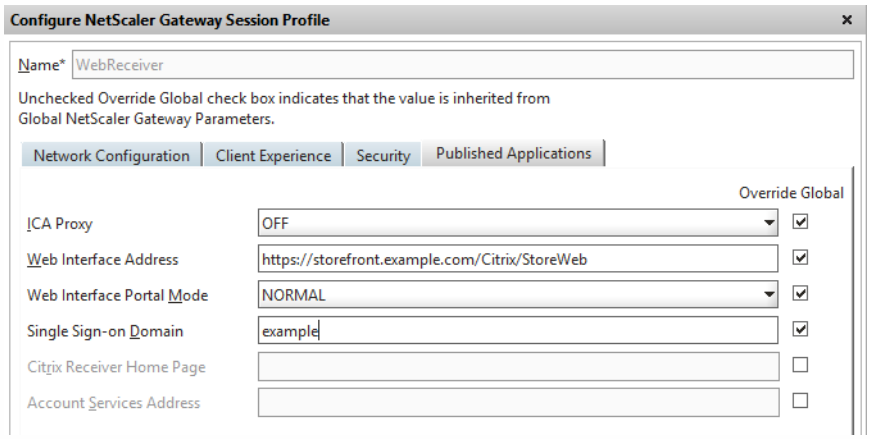
Configure the session profile accounts service URL to be https://accounts.example.com/Citrix/Roaming/Accounts NOT https://storefront.example.com/Citrix/Roaming/Accounts.



Also add this URL as an additional <allowedAudiences> in the authentication and roaming web.config files on the StoreFront server. For more information, see the "Configure the StoreFront server host base URL, gateway, and SSL certificate" section below.

Receiver for Web profile

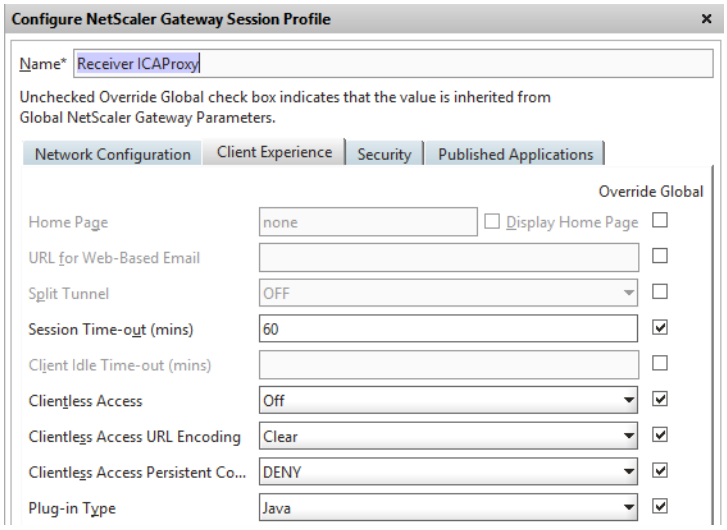


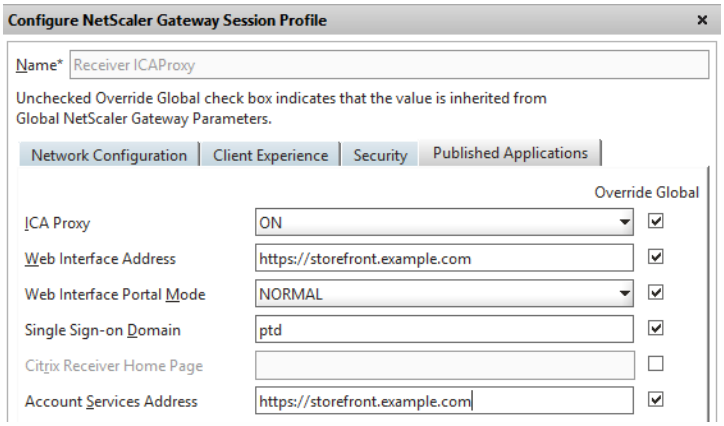


ICA Proxy & Basic Mode settings

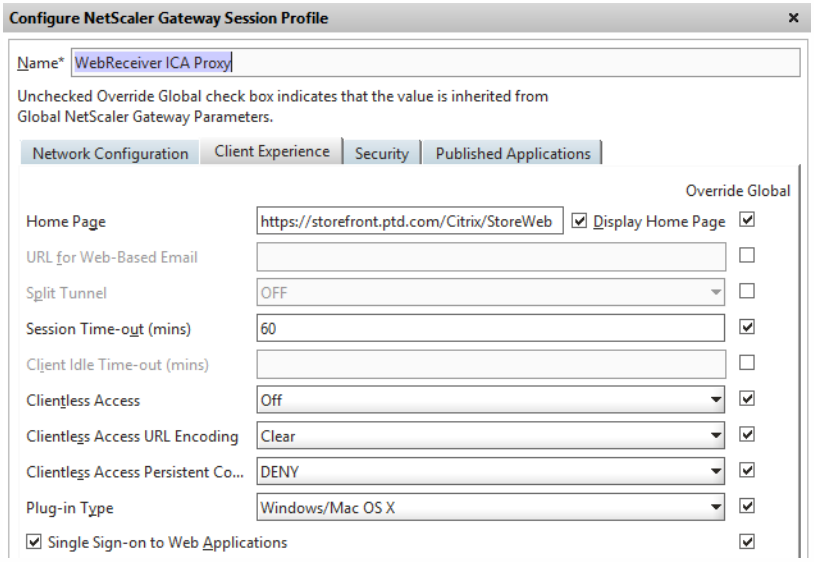
If you use ICA proxy, enable basic mode on the NetScaler Gateway vServer properties page. Only a Netscaler platform license is required.

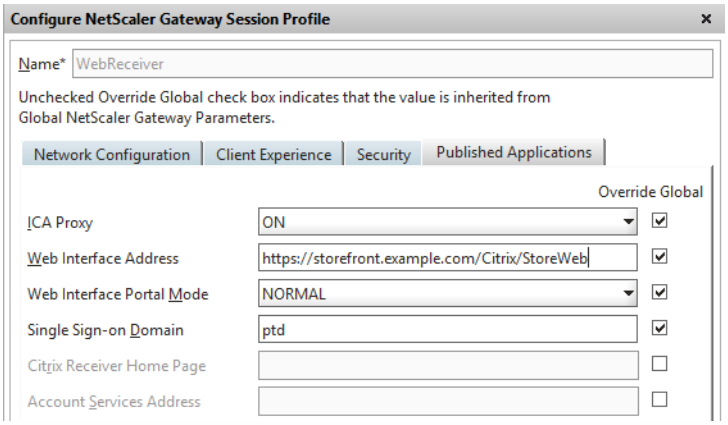
Receiver profile





Receiver for Web profile





Configure the StoreFront server host base URL, gateway, and SSL certificate

The same shared FQDN that resolves to the NetScaler Gateway vServer should also resolve directly to the StoreFront load balancer, if a StoreFront cluster was created or a single StoreFront IP that hosts the store.

Internal DNS: Create three DNS A records.

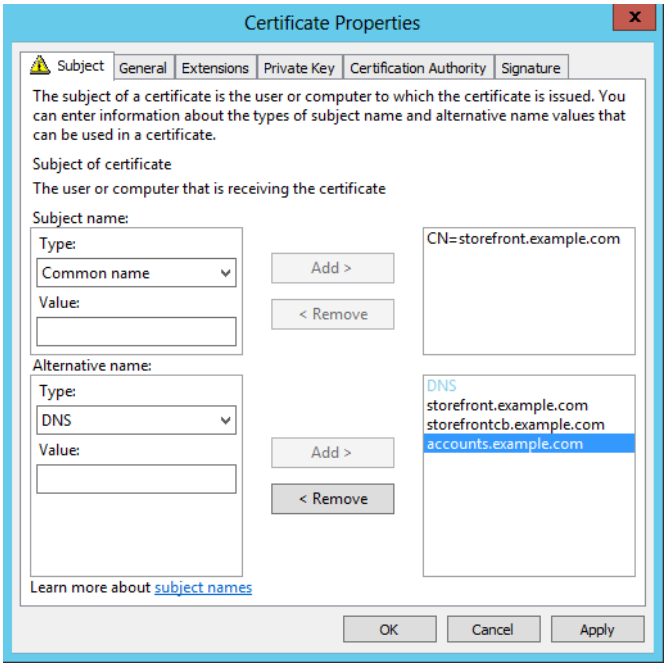
- storefront.example.com should resolve to the storefront load balancer or single StoreFront server IP.
- storefrontcb.example.com should resolve to the gateway vServer VIP so if a firewall exists between the DMZ and the

enterprise local network, allow for this.

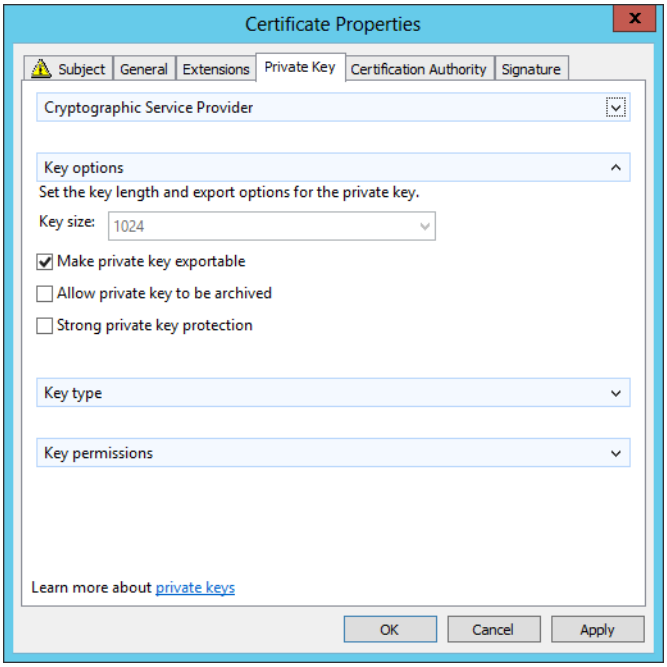
- accounts.example.com — create as a DNS alias for storefront.example.com. It also resolves to the load balancer IP for the StoreFront cluster or a single StoreFront server IP.

StoreFront server example certificate: storefront.example.com

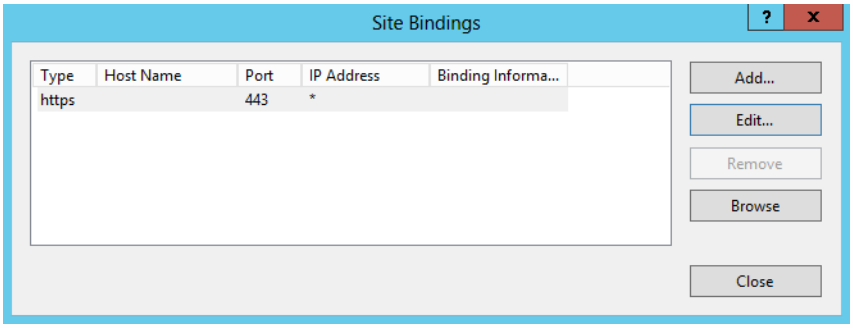
1. Create a suitable certificate for the StoreFront server or server group before installing StoreFront.
2. Add the shared FQDN to the Common name and DNS fields. Ensure this matches the FQDN used in the SSL certificate bound to the NetScaler Gateway vServer that you created earlier or use the same certificate bound to the NetScaler Gateway vServer.
3. Add the accounts alias (accounts.example.com) as another SAN to the certificate. Note that the accounts alias used in the SAN is the one used in the Netscaler Gateway Session Profile in the earlier procedure - **Native Receiver Gateway session policy and profile**.



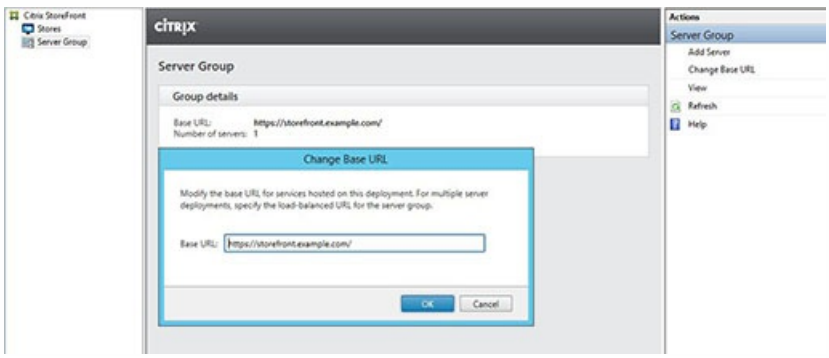
4. Ensure that the private key is exportable so the certificate can be transferred to another server or to multiple StoreFront server group nodes.



5. Sign the certificate using a third party CA such as VeriSign, your enterprise root CA, or intermediate CA.
6. Export the certificate in PFX format including the private key.
7. Import the certificate and private key into the StoreFront server. If deploying a Windows NLB StoreFront cluster, import the certificate into every node. If using an alternative load balancer such as a Netscaler LB vServer, import the certificate there instead.
8. Create an HTTPS binding in IIS on the StoreFront server and bind the imported SSL certificate to it.



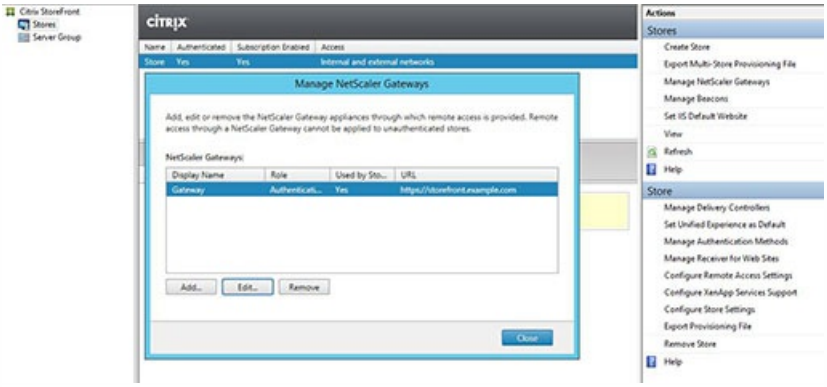
9. Configure the host base URL on the StoreFront server to match the already chosen shared FQDN.
   Note: StoreFront always auto selects the last Subject Alternative Name in the list of SANs within the certificate. This is merely a suggested host base URL to assist StoreFront administrators and is usually correct. You can manually set it to any valid HTTPS://<FQDN> provided it exists within the certificate as a SAN. Example: https://storefront.example.com



Configure the Gateway on the StoreFront server: storefront.example.com

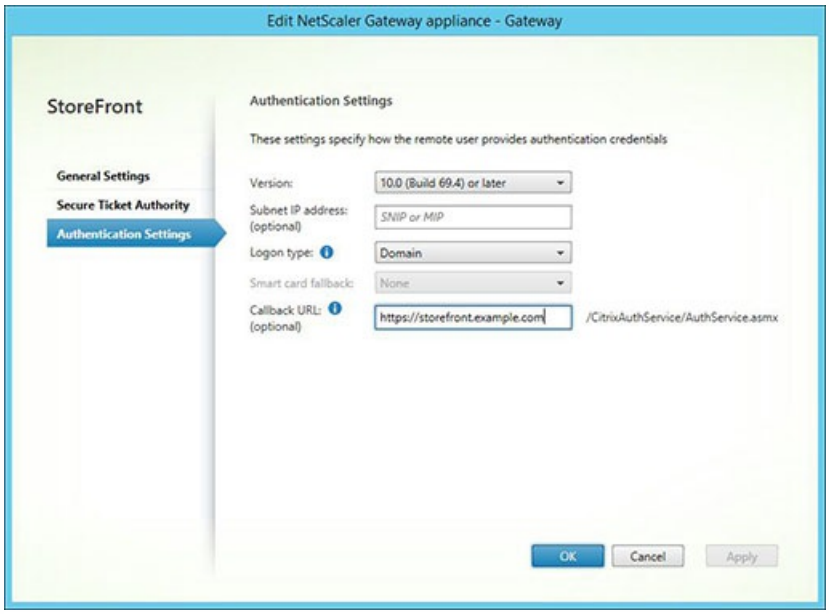
1. From the **Stores** node, click on **Manage NetScaler Gateways** in the **Actions** pane.

2. Select the **Gateway** from the list and click **Edit**.



3. On the **General Settings** page, type the shared FQDN in the **NetScaler Gateway URL** field.

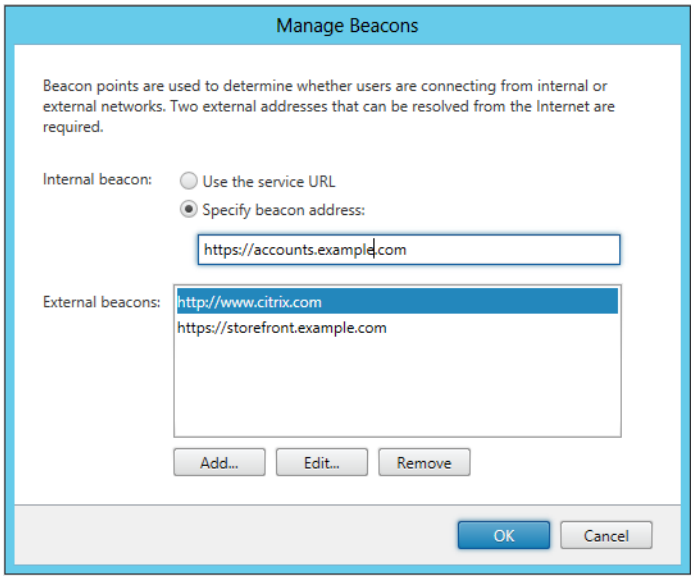
4. Select the **Authentication Settings** tab and type the callback FQDN into the **Callback URL** field.



5. Select the **Secure Ticket Authority** tab and ensure that the Secure Ticket Authority (STA) servers match the list of delivery controllers already configured within the **Store** node.

6. Enable remote access for the store.

7. Manually set the internal beacon to the accounts alias (accounts.example.com) and it must not be resolvable from outside the gateway. This FQDN must be distinct from the external beacon that is shared by the StoreFront hostbase URL and NetScaler Gateway vServer (storefront.example.com). DO NOT use the shared FQDN, as this creates a situation where both the internal and external beacons are identical.



8. Note that if you want to support discovery using FQDNs, follow these steps. If the provisioning file configuration is enough or if you are using only Receiver for Web, you can skip the following steps.

Add an additional <allowedAudiences> entry in C:\inetpub\wwwroot\Citrix\Authentication\web.config. There are two <allowedAudiences> entries in the authentication web.config file. Only the first entry in the file for the Authentication Token Producer requires you to add an additional <allowedAudience>.

9. Perform a search for the <allowedAudiences> string. Locate the following entry below and add the line shown in **bold**, save, and close the web.config file.

<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>
```

9. In **C:\inetpub\wwwroot\Citrix\Roaming\web.config**. Locate the following entry below and add the line shown in **bold**, save, and close the web.config file.

```
<tokenManager>
      <services>
          <clear />
```

.....

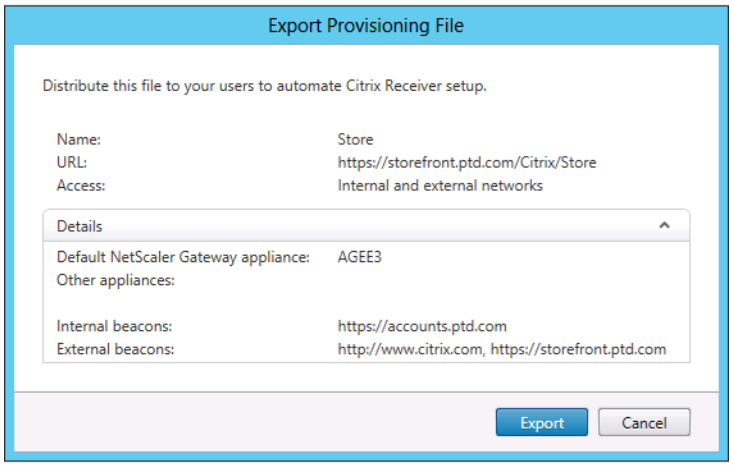
.....

```
            </trustedIssuers>
            <allowedAudiences>
               <add name="https-storefront.example.com" audience="https://storefront.example.com/" />
                    <add name="https-accounts.example.com" audience="https://accounts.example.com/" />
```

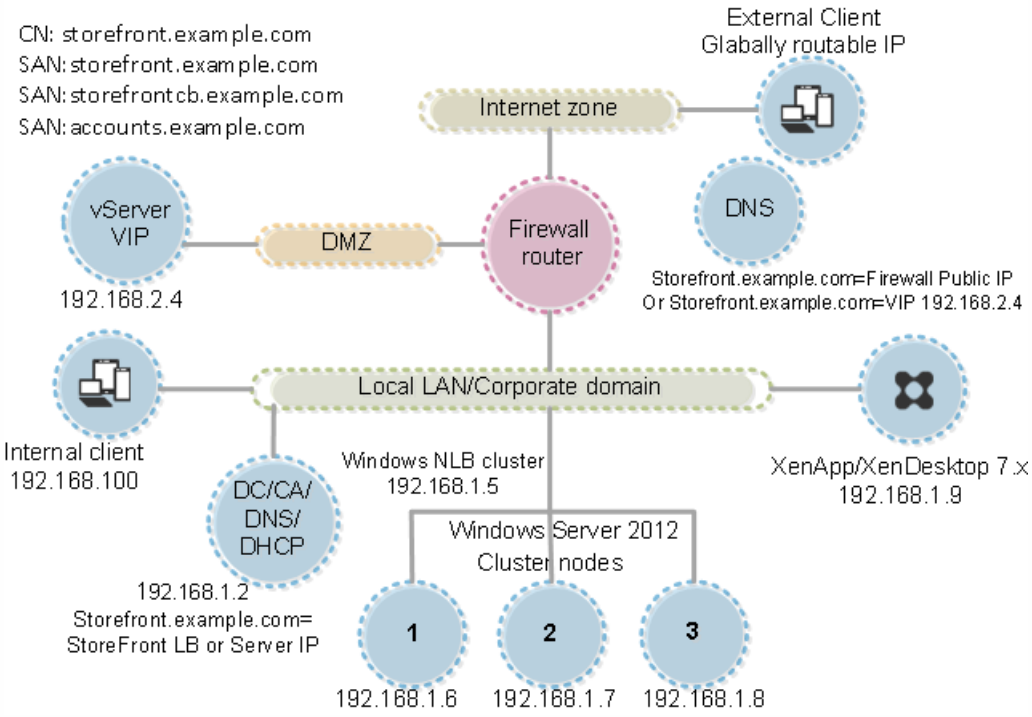


```
    </allowedAudiences>
  </service>
 </services>
</tokenManager>
```

Alternatively, it is possible to export the native receiver .CR provisioning file for the store. This eliminates the need for First Time Use configuration of native Receivers. Distribute this file to all Windows and MAC Receiver clients.



If a Receiver is installed on the client, the .CR file type is recognized and double clicking on the provisioning file triggers it to be automatically imported.



Configure Resource Filtering

May 22, 2017

This topic explains how to filter enumeration resources based on resource type and keywords. You can use this type of filtering with the more advanced customization offered by the Store Customization SDK. Using this SDK, you can control which apps and desktops are displayed to users, modify access conditions, and adjust launch parameters. For more information, see the Store Customization SDK.

Note: The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

Configure filtering

Configure the filter using PowerShell cmdlets defined within the StoresModule. Use the following PowerShell snippet to load the required modules:

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

Filter by type

Use this to filter the resource enumeration by resource type. This is an inclusive filter, meaning it removes any resources that are not of the specified types from the resource enumeration result. Use the following cmdlets:

Set-DSResourceFilterType: Sets up enumeration filtering based on resource types.

Get-DSResourceFilterType: Gets the list of resource types that Storefront is allowed to return in enumeration.

Note: Resource types are applied before keywords.

Filter by keywords

Use this to filter resources based on keywords, such as resources derived from XenDesktop or XenApp. Keywords are generated from mark-up in the description field of the corresponding resource.

The filter can operate either in inclusive or exclusive mode, but not both. The inclusive filter allows enumeration of resources matching the configured keywords and removes non matching resources from the enumeration. The exclusive filter removes resources matching the configured keywords from the enumeration. Use the following cmdlets:

Set-DSResourceFilterKeyword: Sets up enumeration filtering based on resource keywords.

Get-DSResourceFilterKeyword: Gets the list of filter keywords.

The following keywords are reserved and must not be used for filtering:

- Auto
- Mandatory

For more information on keywords, see Optimize the user experience and Configuring application delivery.

Examples

This command will set filtering to exclude workflow resources from enumeration:

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

This example will set allowed resource types to applications only:

```
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -IncludeTypes @("Applications")
```

構成ファイルを使用した構成

May 22, 2017

構成ファイルを使用して、Citrix StoreFront管理コンソールでは設定できないCitrix StoreFrontおよびCitrix Receiver for Webの追加設定を構成できます。

構成できるCitrix StoreFront設定には、次のものがあります。

- ICAファイル署名の有効化
- ファイルタイプの関連付けの無効化
- Citrix Receiverのログオンダイアログボックスのカスタマイズ
- Receiver for Windowsでのパスワードおよびユーザー名のキャッシュ機能の無効化

構成できるCitrix Receiver for Web設定には次のものがあります。

- ユーザーに対するリソースの表示方式
- ［マイアプリケーション］フォルダービューの無効化

Configure StoreFront using the configuration files

May 22, 2017

This article describes additional configuration tasks that cannot be carried out using the Citrix StoreFront management console.

Enable ICA file signing

Disable file type association

Customize the Citrix Receiver logon dialog box

Prevent Citrix Receiver for Windows from caching passwords and usernames

Enable ICA file signing

StoreFront provides the option to digitally sign ICA files so that versions of Citrix Receiver that support this feature can verify that the file originates from a trusted source. When file signing is enabled in StoreFront, the ICA file generated when a user starts an application is signed using a certificate from the personal certificate store of the StoreFront server. ICA files can be signed using any hash algorithm supported by the operating system running on the StoreFront server. The digital signature is ignored by clients that do not support the feature or are not configured for ICA file signing. If the signing process fails, the ICA file is generated without a digital signature and sent to Citrix Receiver, the configuration of which determines whether the unsigned file is accepted.

To be used for ICA file signing with StoreFront, certificates must include the private key and be within the allowed validity period. If the certificate contains a key usage extension, this must allow the key to be used for digital signatures. Where an extended key usage extension is included, it must be set to code signing or server authentication.

For ICA file signing, Citrix recommends using a code signing or SSL signing certificate obtained from a public certification authority or from your organization's private certification authority. If you are unable to obtain a suitable certificate from a certification authority, you can either use an existing SSL certificate, such as a server certificate, or create a new root certification authority certificate and distribute it to users' devices.

ICA file signing is disabled by default in stores. To enable ICA file signing, you edit the store configuration file and execute Windows PowerShell commands. For more information about enabling ICA file signing in Citrix Receiver, see ICA File Signing to protect against application or desktop launches from untrusted servers.

Note: The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.
Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. Ensure that the certificate you want to use to sign ICA files is available in the Citrix Delivery Services certificate store on the StoreFront server and not the current user's certificate store.
2. Use a text editor to open the web.config file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix\storename\ directory, where storename is the name specified for the store when it was created.
3. Locate the following section in the file.

```
<certificateManager>
  <certificates>
    <clear />
    <add ... />
    ...
  </certificates>
</certificateManager>
```

4. Include details of the certificate to be used for signing as shown below.

```
<certificateManager>
  <certificates>
    <clear />
    <add id="certificateid" thumb="certificatethumbprint" />
    <add ... />
    ...
  </certificates>
</certificateManager>
```

   Where certificateid is a value that helps you to identify the certificate in the store configuration file and certificatethumbprint is the digest (or thumbprint) of the certificate data produced by the hash algorithm.

5. Locate the following element in the file.

```
<icaFileSigning enabled="False" certificateId="" hashAlgorithm="sha1" />
```

6. Change the value of the enabled attribute to True to enable ICA file signing for the store. Set the value of the certificateId attribute to the ID you used to identify the certificate, that is, certificateid in Step 4.
7. If you want to use a hash algorithm other than SHA-1, set the value of the hashAgorithm attribute to sha256, sha384, or sha512, as required.
8. Using an account with local administrator permissions, start Windows PowerShell and, at a command prompt, type the following commands to enable the store to access the private key.

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
 $certificate = Get-DSCertificate "certificatethumbprint"
```

Add-DSCertificateKeyReadAccess -certificate $certificates[0] -accountName “IIS APPPOOL\Citrix Delivery Services Resources”
Where certificatethumbprint is the digest of the certificate data produced by the hash algorithm.

Disable file type association

By default, file type association is enabled in stores so that content is seamlessly redirected to users' subscribed applications when they open local files of the appropriate types. To disable file type association, you edit the store configuration file.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. Use a text editor to open the web.config file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix\storename\ directory, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.
   <farmset ... enableFileTypeAssociation="on" ... >
3. Change the value of the enableFileTypeAssociation attribute to off to disable file type association for the store.

Customize the Citrix Receiver logon dialog box

When Citrix Receiver users log on to a store, no title text is displayed on the logon dialog box, by default. You can display the default text “Please log on” or compose your own custom message. To display and customize the title text on the Citrix Receiver logon dialog box, you edit the files for the authentication service.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. Use a text editor to open the UsernamePassword.tfrm file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\ directory.
2. Locate the following lines in the file.
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
3. Uncomment the statement by removing the leading and trailing leading @* and trailing *@, as shown below.
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   Citrix Receiver users see the default title text “Please log on”, or the appropriate localized version of this text, when they log on to stores that use this authentication service.
4. To modify the title text, use a text editor to open the ExplicitAuth.resx file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\ directory.
5. Locate the following elements in the file. Edit the text enclosed within the <value> element to modify the title text that users see on the Citrix Receiver logon dialog box when they access stores that use this authentication service.
   <data name="AuthenticateHeadingText" xml:space="preserve">
   <value>My Company Name</value>
   </data>
   To modify the Citrix Receiver logon dialog box title text for users in other locales, edit the localized files ExplicitAuth.languagecode.resx, where languagecode is the locale identifier.

Prevent Citrix Receiver for Windows from caching passwords and usernames

By default, Citrix Receiver for Windows stores users' passwords when they log on to StoreFront stores. To prevent Citrix Receiver for Windows, but not Citrix Receiver for Windows Enterprise, from caching users' passwords, you edit the files for the authentication service.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

1. Use a text editor to open the inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrm file.
2. Locate the following line in the file.
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))
3. Comment the statement as shown below.
   <!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials")) -->
   Citrix Receiver for Windows users must enter their passwords every time they log on to stores that use this authentication service. This setting does not apply to Citrix Receiver for Windows Enterprise.

> **警告**
>
> Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

By default, Citrix Receiver for Windows automatically populated the last username entered. To supress population of the username field, edit the registry on the user device:

1. Create a REG_SZ value HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Set its value “false”.

構成ファイルを使ったCitrix Receiver for Webサイトの構成

May 22, 2017

ここでは、Citrix StoreFront管理コンソールを使用して実行できない、Citrix Receiver for Webサイトの付加的な構成タスクについて説明します。

ユーザーに対するリソースの表示方式の構成

Citrix Receiver for Webサイトからデスクトップとアプリケーションの両方にアクセスできる場合、デフォルトでデスクトップとアプリケーションが別々のビューで表示されます。サイトにログオンすると、最初にデスクトップビューが表示されます。ユーザーがアクセスできるデスクトップが1つのみの場合、アクセス可能なアプリケーションがあるかどうかにかかわらず、ユーザーのログオン時にそのデスクトップが自動的に起動します。これらの設定を変更するには、サイトの構成ファイルを編集します。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってCitrix Receiver for Webサイトのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storenameWeb\フォルダーにあります。ここで、storenamestorenameはストアの作成時に指定した名前です。
2. ファイル内で次の要素を検索します。

3. ユーザーがアクセス可能なデスクトップやアプリケーションを非表示にするには、showDesktopsView属性（デスクトップ）およびshowAppsView属性（アプリケーション）の値をfalseに変更します。デスクトップビューとアプリケーションビューの両方が有効な場合は、defaultView属性の値をappsに設定すると、ユーザーがサイトにログオンしたときに最初にアプリケーションビューが表示されます。
4. ファイル内で次の要素を検索します。

5. デスクトップの自動起動を無効にするには、autoLaunchDesktop属性の値をfalseに変更します。これにより、ユーザーがアクセスできるデスクトップが1つのみの場合でも、ログオン時にデスクトップが自動的に起動しなくなります。autoLaunchDesktop属性がtrueの場合、使用可能なデスクトップが1つのみのユーザーがログオンしてもアプリケーションには再接続されません（ワークスペースコントロールが有効になっていても再接続されません）。

注：Citrix Receiver for Webサイトによるデスクトップの自動起動を有効にするには、Internet Explorerでサイトにアクセスするユーザーは［ローカルイントラネット］または［信頼済みサイト］のゾーンにサイトを追加する必要があります。

［マイアプリケーション］フォルダービューの無効化

Citrix Receiver for Webのデフォルトでは、認証不要なストア（匿名ユーザー用）と必須ストア（ユーザーがサブスクライブしなくてもすべての公開アプリケーションがホーム画面に追加される）の［マイアプリケーション］フォルダービューが表示されます。このビューにはアプリケーションがフォルダー階層で表示され、フォルダーパスの情報も表示されます。

重要：複数サーバーによる展開環境では、複数のサーバー上で同時にサーバーグループの構成を変更しないでください。展開内のほかのサーバー上でCitrix StoreFront管理コンソールを同時に実行していないことを確認してください。変更が完了したら、構成の変更をサーバーグループに反映させて、展開内のほかのサーバーを更新します。

1. テキストエディターを使ってCitrix Receiver for Webサイトのweb.configファイルを開きます。このファイルは通常、C:\inetpub\wwwroot\Citrix\storenameWeb\フォルダーにあります。ここで、storenameはストアの作成時に指定した名

前です。

2. ファイル内で次の要素を検索します。
3. enableAppsFolderView属性の値をfalseに変更します。これにより、Citrix Receiver for Webの［マイアプリケーション］フォルダービューが無効になります。

Secure your StoreFront deployment

May 22, 2017

This article highlights areas that may have an impact on system security when deploying and configuring StoreFront.

Configure Microsoft Internet Information Services (IIS)

You can configure StoreFront with a restricted IIS configuration. Note that this is not the default IIS configuration.

Filename extensions

You can disallow unlisted file name extensions.

StoreFront requires these file name extensions in Request Filtering:

- . (blank extension)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .gif
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

If download or upgrade of Citrix Receiver is enabled for Citrix Receiver for Web, StoreFront also requires these file name extensions:

- .dmg
- .exe

If Citrix Receiver for HTML5 is enabled, StoreFront also requires these file name extensions:

- .eot
- .ttf
- .woff

StoreFront requires the following HTTP verbs in Request Filtering. You can disallow unlisted verbs.

- GET
- POST
- HEAD

StoreFront does not require:

- ISAPI filters
- ISAPI extensions
- CGI programs
- FastCGI programs

> **Important**
>
> - StoreFront requires Full Trust. Do not set the global .NET trust level to High or lower.
> - StoreFront does not support a separate application pool for each site. Do not modify these site settings.

Configure user rights

When you install StoreFront, its application pools are granted the logon right **Log on as a service** and the privileges **Adjust memory quotas for a process, Generate security audits**, and **Replace a process level token**. This is normal installation behavior when application pools are created.

You do not need to change these user rights. These privileges are not used by StoreFront and are automatically disabled.

StoreFront installation creates the following Windows services:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)
- Citrix Peer Resolution (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Credential Wallet (NT SERVICE\CitrixCredentialWallet)
- Citrix Subscriptions Store (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Default Domain Services (NT SERVICE\CitrixDefaultDomainService)

If you configure StoreFront Kerberos constrained delegation for XenApp 6.5, this creates the Citrix StoreFront Protocol Transition service (NT SERVICE\SYSTEM). This service requires a privilege not normally granted to Windows services.

Configure service settings

The StoreFront Windows services listed above in the "Configure user rights" section are configured to log on as the NETWORK SERVICE identity. The Citrix StoreFront Protocol Transition service logs on as SYSTEM. Do not change this configuration.

Configure group memberships

StoreFront installation adds the following services to the Administrators security group:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)

These group memberships are required for StoreFront to operate correctly, to:

- Create, export, import and delete certificates, and set access permissions on them
- Read and write the Windows registry

- Add and remove Microsoft .NET Framework assemblies in the Global Assembly Cache (GAC)
- Access the folder **Program Files\Citrix**<*StoreFrontLocation*>
- Add, modify, and remove IIS app pool identities and IIS web applications
- Add, modify, and remove local security groups and firewall rules
- Add and remove Windows services and PowerShell snap-ins
- Register Microsoft Windows Communication Framework (WCF) endpoints

In updates to StoreFront, this list of operations might change without notice.

StoreFront installation also creates the following local security groups:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSUsers
- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront maintains the membership of these security groups. They are used for access control within StoreFront, and are not applied to Windows resources such as files and folders. Do not modify these group memberships.

Certificates in StoreFront

Server certificates

Server certificates are used for machine identification and Transport Layer Security (TLS) transport security in StoreFront. If you decide to enable ICA file signing, StoreFront can also use certificates to digitally sign ICA files.

To enable email-based account discovery for users installing Citrix Receiver on a device for the first time, you must install a valid server certificate on the StoreFront server. The full chain to the root certificate must also be valid. For the best user experience, install a certificate with a Subject or Subject Alternative Name entry of **discoverReceiver.domain**, where domain is the Microsoft Active Directory domain containing your users' email accounts. Although you can use a wildcard certificate for the domain containing your users' email accounts, you must first ensure that the deployment of such certificates is permitted by your corporate security policy. Other certificates for the domain containing your users' email accounts can also be used, but users will see a certificate warning dialog box when Citrix Receiver first connects to the StoreFront server. Email-based account discovery cannot be used with any other certificate identities. For more information, see Configure email-based account discovery.

If your users configure their accounts by entering store URLs directly into Citrix Receiver and do not use email-based account discovery, the certificate on the StoreFront server need only be valid for that server and have a valid chain to the root certificate.

Token management certificates

Authentication services and stores each require certificates for token management. StoreFront generates a self-signed certificate when an authentication service or store is created. Self-signed certificates generated by StoreFront should not

be used for any other purpose.

Citrix Delivery Services certificates

StoreFront holds a number of certificates in a custom Windows certificate store (Citrix Delivery Services). The Citrix Configuration Replication service, Citrix Credential Wallet service, and Citrix Subscriptions Store service use these certificates. Each StoreFront server in a cluster has a copy of these certificates. These services do not rely on TLS for secure communications, and these certificates are not used as TLS server certificates. These certificates are created when a StoreFront store is created or StoreFront is installed. Do not modify the contents of this Windows certificate store.

Code signing certificates

StoreFront includes a number of PowerShell scripts (.ps1) in the folder in <InstallDirectory>\Scripts. The default StoreFront installation does not use these scripts. They simplify the configuration steps for specific and infrequent tasks. These scripts are signed, allowing StoreFront to support PowerShell execution policy. We recommend the **AllSigned** policy. (The **Restricted** policy is not supported, as this prevents PowerShell scripts from executing.) StoreFront does not alter the PowerShell execution policy.

Although StoreFront does not install a code signing certificate in the Trusted Publishers store, Windows can automatically add the code signing certificate there. This happens when the PowerShell script is executed with the **Always run** option. (If you select the **Never run** option, the certificate is added to the Untrusted Certificates store, and StoreFront PowerShell scripts will not execute.) Once the code signing certificate has been added to the Trusted Publishers store, its expiration is no longer checked by Windows. You can remove this certificate from the Trusted Publishers store after the StoreFront tasks have been completed.

StoreFront communications

In a production environment, Citrix recommends using the Internet Protocol security (IPsec) or HTTPS protocols to secure data passing between StoreFront and your servers. IPsec is a set of standard extensions to the Internet Protocol that provides authenticated and encrypted communications with data integrity and replay protection. Because IPsec is a network-layer protocol set, higher level protocols can use it without modification. HTTPS uses the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to provide strong data encryption.

The SSL Relay can be used to secure data traffic between StoreFront and XenApp servers. The SSL Relay is a default component of XenApp that performs host authentication and data encryption.

Citrix recommends securing communications between StoreFront and users' devices using NetScaler Gateway and HTTPS. To use HTTPS, StoreFront requires that the Microsoft Internet Information Services (IIS) instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications. Citrix strongly recommends that you do not enable unsecured user connections to StoreFront in a production environment.

StoreFront security separation

If you deploy any web applications in the same web domain (domain name and port) as StoreFront, then any security risks in those web applications could potentially reduce the security of your StoreFront deployment. Where a greater degree of security separation is required, Citrix recommends that you deploy StoreFront in a separate web domain.

ICA file signing

StoreFront provides the option to digitally sign ICA files using a specified certificate on the server so that versions of Citrix

Receiver that support this feature can verify that the file originates from a trusted source. ICA files can be signed using any hash algorithm supported by the operating system running on the StoreFront server, including SHA-1 and SHA-256. For more information, see Enable ICA file signing.

User change password

You can enable Receiver for Web site users logging on with Active Directory domain credentials to change their passwords, either at any time or only when they have expired. However, this exposes sensitive security functions to anyone who can access any of the stores that use the authentication service. If your organization has a security policy that reserves user password change functions for internal use only, ensure that none of the stores are accessible from outside your corporate network. When you create the authentication service, the default configuration prevents Receiver for Web site users from changing their passwords, even if they have expired. For more information, see Optimize the user experience.

Customizations

To strengthen security, do not write customizations that load content or scripts from servers not under your control. Copy the content or script into the Citrix Receiver for Web site custom folder where you are making the customizations. If StoreFront is configured for HTTPS connections, ensure that any links to custom content or scripts also use HTTPS.

Export and import the StoreFront configuration

May 22, 2017

You can export the entire configuration of a StoreFront deployment. This includes both single server deployments and server group configurations. If an existing deployment is already present on the importing server, the current configuration is erased and then replaced by the configuration contained within the backup archive. If the target server is a clean factory default installation, a new deployment is created using the imported configuration stored within the backup. The exported configuration backup is in the form of a single .zip archive if unencrypted, or a .ctxzip if you choose to encrypt the backup file when it is created.

Things to consider when exporting and importing a StoreFront configuration

- Do you want to use the Host Base URL contained in the backup archive or specify a new Host Base URL to use on the importing server?
- Do you currently use any Citrix published authentication SDK examples, such as Magic Word authentication or third party authentication customizations? If so, you must install these packages on ALL importing servers BEFORE importing a configuration containing extra authentication methods. The configuration import fails if required authentication SDK packages are not installed on any of the importing servers. If importing a configuration into a server group, install the authentication packages on all members of the group.
- You can encrypt or decrypt your configuration backups. The exporting and importing PowerShell cmdlets support both use cases.
- You can decrypt encrypted backups (.ctxzip) later, but StoreFront cannot re-encrypt unencrypted backup files (.zip). If an encrypted backup is required, perform the export again using a PowerShell credential object containing a password of your choice.
- The SiteID of the website in IIS where StoreFront is currently installed (exporting server) must match the SiteID of the target website in IIS (importing server) where you want to restore the backed up StoreFront configuration.

PowerShell credential objects used for encryption and decryption of StoreFront backups

A PowerShell credential object comprises both a Windows account username and a password. PowerShell credential objects ensure that your password stays protected in memory.

> **注意**
>
> To encrypt a configuration backup archive, you need only the password to perform encryption and decryption. The username stored within the credential object is not used. You must create a credential object containing the same password within the PowerShell sessions that is used **on both the exporting and importing servers**. Within the credential object you can specify any user.

PowerShell requires that you specify a user when creating a new credential object. This example code obtains only the currently logged on Windows user for convenience.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
```

PowerShell cmdlets

Export-STFConfiguration

Parameter	Description
-TargetFolder (String)	The export path to the backup archive. Example: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Specify a credential object to create an encrypted .ctxzip backup archive during export. The PowerShell credential object should contain the password to use for encryption and decryption. Do not use **-Credential** at the same time as the **-NoEncryption** parameter. Example: $CredObject
-NoEncryption (Switch)	Specify that the backup archive should be an unencrypted .zip. Do not use **-NoEncryption** at the same time as the **-Credential** parameter.
-ZipFileName (String)	The name for the StoreFront configuration backup archive. Do not add a file extension, such as .zip or .ctxzip. The file extension is added automatically depending on whether the **-Credential** or **-NoEncryption** parameter is specified during export. Example: "backup"
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.

Important

The **-SiteID** parameter found in StoreFront 3.5 was deprecated in version 3.6. It is no longer necessary to specify the **SiteID** when performing an import, as the SiteID contained within the backup archive is always be used. Ensure the SiteID matches the existing StoreFront website already configured within IIS on the importing server. **SiteID 1** to **SiteID 2** (or vice versa) configuration imports are NOT supported.

Import-STFConfiguration

Parameter	Description
-ConfigurationZip (String)	The full path to the backup archive you want to import. This should also include the file extension. Use .zip for unencrypted and .ctxzip for encrypted backup archives. Example: "$env:userprofile\desktop\backup.ctxzip"
-Credential (PSCredential Object)	Specify a credential object to decrypt an encrypted backup during import. Example: $CredObject
-HostBaseURL (String)	If this parameter is included, the Host base URL you specify is used instead of the Host base URL from the exporting server. Example: "https://<importingserver>.example.com"

Unprotect-STFConfigurationBackup

Parameter	Description
-TargetFolder (String)	The export path to the backup archive. Example: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Use this parameter to create an unencrypted copy of the encrypted backup archive. Specify the PowerShell credential object containing the password to use for decryption. Example: $CredObject
-EncryptedConfigurationZip (String)	The full path of the encrypted backup archive you want to decrypt. You must specify the file extension .ctxzip. Example: "$env:userprofile\desktop\backup.ctxzip"
-OutputFolder (String)	The path to create an unencrypted copy (.zip) of the encrypted (.ctxzip) backup archive. The original encrypted copy of the backup is retained so it can be reused. Do not specify a file name and file extension for the unencrypted copy. Example: "$env:userprofile\desktop\"
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as

existing backup files already present in the specified export location.

Configuration export and import examples

Import the StoreFront SDK into the current PowerShell session

Open the PowerShell Integrated Scripting Environment (ISE) on the StoreFront server and run:

```
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
Import-Module "$SDKModules.SubscriptionsStore\Citrix.StoreFront.SubscriptionsStore.psd1" -verbose
```

Single server scenarios

Create an unencrypted backup of an existing configuration on Server A and restore it onto the same deployment.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -NoEncryption
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.zip"
```

Create an encrypted backup of an existing configuration on Server A and restore it onto the same deployment.

```
# Create a PowerShell Credential Object
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -Credential $CredObject
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

Unprotect an existing encrypted backup archive

```
$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
```

Back up an existing configuration on Server A and restore it onto a new factory default installation on Server B

Server B is a new deployment but intended to coexist alongside Server A. Specify the **-HostBaseURL** parameter. Server B is

also a new factory default StoreFront installation.

1. Create a PowerShell credential object and export an encrypted copy of the Server A configuration.
2. Create a PowerShell credential object on Server B using the same password you used to encrypt the backup.
3. Decrypt and import the Server A configuration onto Server B using the **-HostBaseURL** parameter.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://serverB.example.com
```

Back up an existing configuration on Server A and use it to overwrite an existing deployment on Server B

Server B is an existing deployment with an outdated configuration. Use the Server A configuration to update Server B. Server B is intended to coexist alongside Server A. Specify the **-HostBaseURL** parameter.

1. Create a PowerShell credential object and export an encrypted copy of the Server A configuration.
2. Create a PowerShell credential object on Server B using the same password you used to encrypt the backup.
3. Decrypt and import the Server A configuration onto Server B using the **-HostBaseURL** parameter.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

Create a clone of an existing deployment with the same host base URL such as when upgrading to a new server OS and decommissioning an obsolete StoreFront deployment

2012R2 Server B is a new deployment intended to replace the obsolete 2008R2 Server A. Use the HostBaseURL from within the backup archive. Do not use the **-HostBaseURL** parameter during import. Server B is also a new factory default StoreFront installation.

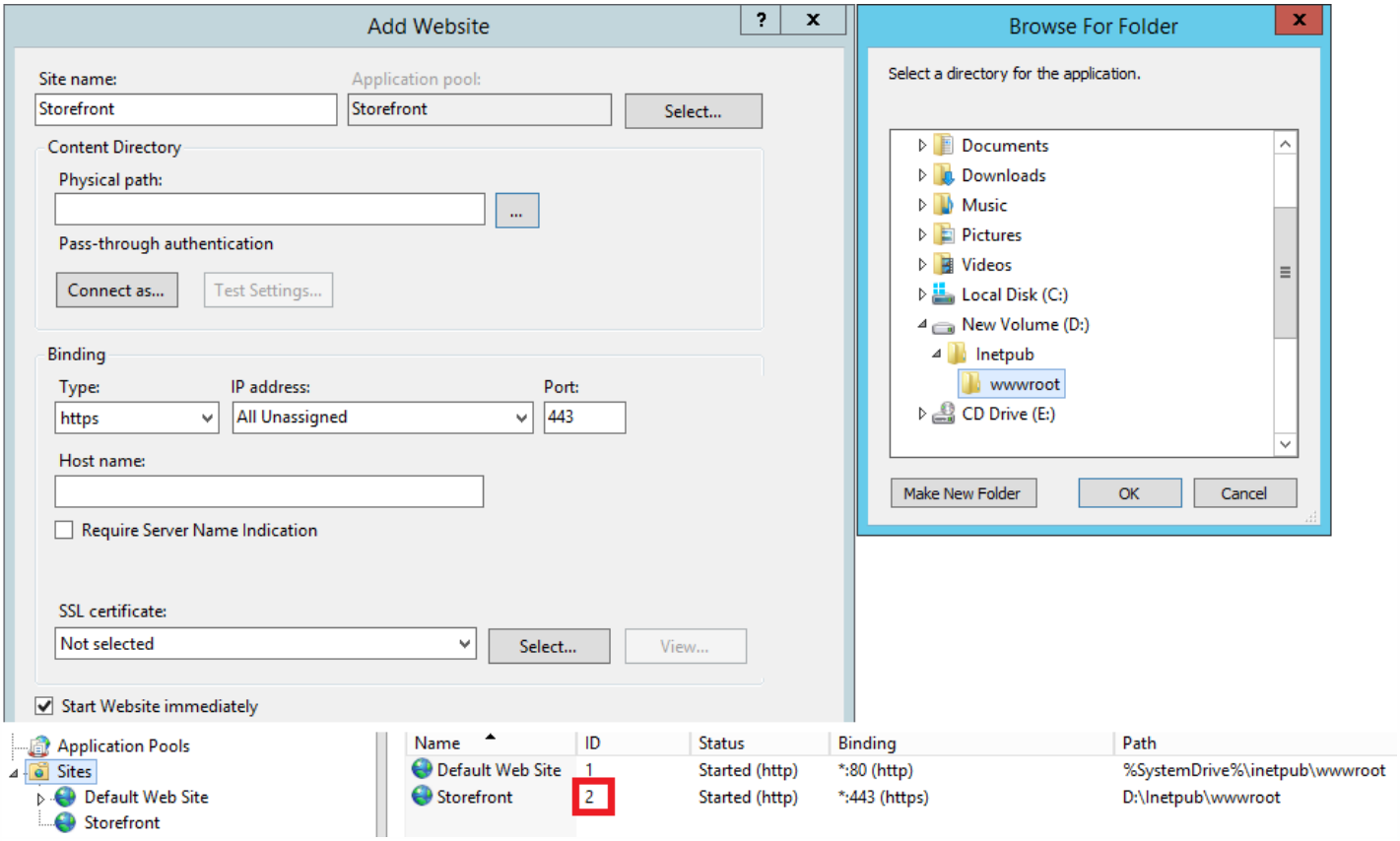
1. Create a PowerShell credential object and export an encrypted copy of the 2008R2 Server A configuration.
2. Create a PowerShell credential object on 2012R2 Server B using the same password you used to encrypt the backup.
3. Decrypt and import the 2008R2 Server A configuration onto 2012R2 Server B without using the **-HostBaseURL** parameter.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

StoreFront is already deployed onto a custom website in IIS. Restore the configuration onto another custom website deployment.

Server A has StoreFront deployed on a custom website location rather than the usual default website within IIS. The IIS SiteID for the second website created in IIS is 2. The StoreFront website's physical path can be on another nonsystem drive such as d:\ or on the default c:\ system drive but should use an IIS SiteID greater than 1.

A new website called StoreFront has been configured within IIS, which uses **SiteID = 2**. StoreFront is already deployed on the custom website in IIS with its physical path on drive d:\inetpub\wwwrooot\.



1. Create a PowerShell credential object and export an encrypted copy of the Server A configuration.
2. On Server B, configure IIS with a new website called **StoreFront**, which also uses **SiteID 2**.
3. Create a PowerShell credential object on Server B using the same password you used to encrypt the backup.
4. Decrypt and import the Server A configuration onto Server B using the **-HostBaseURL** parameter. The site ID contained in the backup is used and must match the target website where you want to import the StoreFront configuration.

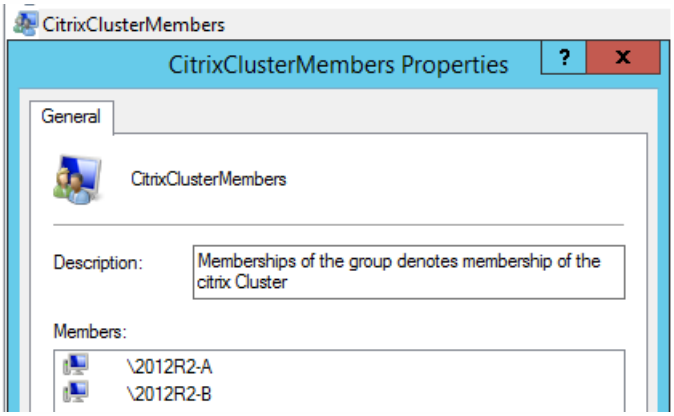
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -HostBaseURL "https://serverB.example.com"
```

Server group scenarios

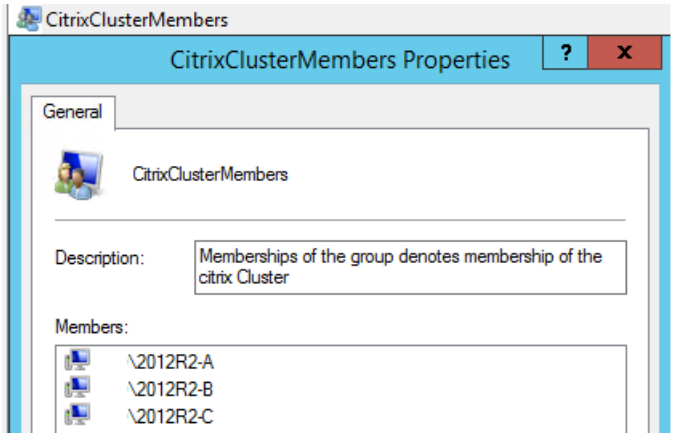
Scenario 1: Backup an existing server group configuration and restore it later onto the same server group deployment.

A previous configuration backup was taken while only two StoreFront servers, 2012R2-A and 2012R2-B, were members of the server group. Within the backup archive is a record of the **CitrixClusterMembership** at the time the backup was taken containing only the two original servers 2012R2-A and 2012R2-B. The StoreFront server group deployment has subsequently increased in size since the original backup was taken due to business demand, so an additional node 2012R2-C has been added to the server group. The underlying StoreFront configuration of the server group held in the backup has not changed. The current CitrixClusterMembership of three servers must be maintained even if an old backup containing only the two original server group nodes is imported. During import the current cluster membership is preserved and then written back once the configuration has been successfully imported onto the primary server. The import also preserves the current CitrixClusterMembership if server group nodes were removed from the server group since the original backup was taken.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.



2. Later you add an additional server, 2012R2-C to the existing server group.



3. The configuration of the server group must be restored to a known previously working state. StoreFront backs up the current CitrixClusterMembership of three servers during the import process, and then restores it after the import has succeeded.

4. Import the Server Group 1 configuration back onto node 2012R2-A.

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject

5. Propagate the newly imported configuration to the entire server group, so all servers have a consistent configuration after import.

Scenario 2: Backup an existing configuration from Server Group 1 and use it to create a new Server Group on a different factory default installation. You can then add other new server group members to the new primary server.

Server Group 2 is created containing two new servers, 2012R2-C and 2012R2-D. The Server Group 2 configuration will be based on the configuration of an existing deployment, Server Group 1, which also contains two servers 2012R2-A and 2012R2-B. The CitrixClusterMembership contained within the backup archive is not used when creating a new server group.

The current CitrixClusterMembership is always backed up and then restored after the import is successful. When creating a new deployment using an imported configuration, the CitrixClusterMembership security group contains only the importing server until additional servers are joined to the new group. Server Group 2 is a new deployment and intended to coexist alongside Server Group 1. Specify the -HostBaseURL parameter. Server Group 2 will be created using a new factory default StoreFront installation.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.

2. Import the Server Group 1 configuration onto node 2012R2-C, which will be the primary server used to manage the newly created Server Group 2.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://servergroup2.example.com"
```

3. Join any additional servers that will be part of the new Server Group 2 deployment. Propagation of the newly imported configuration from Server Group 1 to all new members of Server Group 2 is automatic, as this forms part of the normal join process when a new server is added.

Scenario 3: Backup an existing configuration from Server Group A and use it to overwrite the existing Server Group B configuration.

Server Group 1 and Server Group 2 already exist in two separate data centers. Many StoreFront configuration changes are made on Server Group 1, which you should apply to Server Group 2 in the other data center. You can port the changes from Server Group 1 to Server Group 2. Do not use the **CitrixClusterMembership** within the backup archive on Server Group 2. Specify the **-HostBaseURL** parameter during import, as the Server Group 2 host base URL should not be changed to the same FQDN that is currently in use by Server Group 1. Server Group 2 is an existing deployment.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.

2. Import the Server Group 1 configuration onto the factory default installation on node 2012R2-C, which will be the primary server of the new Server Group 2.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://servergroup2.example.com"
```

StoreFront SDK

May 22, 2017

Citrix StoreFront provides an SDK based on a number of Microsoft Windows PowerShell version 3.0 modules. With the SDK, you can perform the same tasks as you would with the StoreFront MMC console, together with tasks you cannot do with the console alone.

For the SDK Reference, see StoreFront SDK.

Key differences between the StoreFront 3.0 and current StoreFront SDK

- **High-level SDK Examples** - This version provides high-level SDK scripts that enable you to script and automate StoreFront deployments quickly and easily. You can tailor the high-level examples to your particular requirements enabling you to create a new deployment simply by running one script.
- **New low-level SDK** - Citrix provides a documented low-level StoreFront SDK enabling the configuration of deployments including stores, authentication methods, Citrix Receiver for Web and Unified Citrix Receiver sites, as well as remote access with NetScaler Gateway.
- **Backwards Compatibility** - StoreFront 3.6 still contains the StoreFront 3.0 and earlier APIs so existing scripts can be gradually transitioned to the new SDK.

Important

Backwards compatibility with StoreFront 3.0 has been maintained where possible and practicable. However, Citrix recommends when writing new scripts, use the new **Citrix.StoreFront.*** modules, as the StoreFront 3.0 SDK is deprecated and will eventually be removed.

Use the SDK

The SDK comprises of a number of PowerShell snap-ins installed automatically by the installation wizard when you install and configure various StoreFront components.

To access and run the cmdlets:

1. Start a shell in PowerShell 3.0.
   You must run the shell or script using a member of the local administrators group on the StoreFront server.

2. To use SDK cmdlets within scripts, set the execution policy in PowerShell.
   For more information about PowerShell execution policy, see your Microsoft documentation.

3. Add the modules you require into the PowerShell environment using the **Add -Module** command in the Windows PowerShell console. For example, type:
   Import-Module Citrix.StoreFront
   To import all the cmdlets, type:

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront") } | Import-Module
   ```

After importing, you have access to the cmdlets and their associated help.

Get started with the SDK

To create a script, perform the following steps:

1. Take one of the provided SDK examples installed by StoreFront into the **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** folder.
2. To help you customize your own script. review the example script to understand what each part is doing. For more information, see the example use case, which explains in detail the script's actions.
3. Convert and adapt the example scripts to turn them into a script that is more consumable. To do this:
   - Use the PowerShell ISE or a similar tool to edit the script.
   - Use variables to assign values that are to be reused or modified.
   - Remove any commands that are not required.
   - Note that StoreFront cmdlets can be identified by the prefix STF.
   - Use the Get-Help cmdlet supplying the cmdlet name and -Full parameter for more information on a specific command.

Examples

Note: When creating a script, to ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described above rather than copying and pasting the example scripts.

Examples	Description
<Example: Create a Simple Deployment>	Script: creates a simple deployment with a StoreFront controller configured with a single XenDesktop server.
<Example: Create a Remote Access Deployment>	Script: builds on the previous script to add remote access to the deployment.
<Example: Create a Remote Access Deployment with Optimal Launch Gateway>	Script: builds on the previous script to add preferred optimal launch gateways for a better user experience.
<Example: Create a Deployment with a Desktop Appliance Site>	Script: creates a simple deployment configured with a Desktop Appliance site.

Example: Create a simple deployment

The following example shows how to create a simple deployment configured with one XenDesktop controller.

Before you begin, make sure you follow the steps detailed in Get Started with the SDK. This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and imports the required StoreFront modules. Imports are not required in newer versions of PowerShell.

```
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
```

- Automates the virtual path of the authentication and Citrix Receiver for Web services based on the **$StoreVirtualPath** supplied.

```
# Determine the Authentication and Receiver virtual path to use based of the Store

$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"

$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
```

- Creates a new deployment if one is not already present iin preparation for adding the required StoreFront services. **-Confirm:$false** supresses the requirement to confirm the deployment can procede.

```
# 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."

}
```

- Creates a new authentication service if one does not exist at the specified virtual path. The default authentication method of username and password is enabled.

```
# Determine if the authentication service at the specified virtual path exists

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

if(-not $authentication)

{

   # Add an Authentication service using the IIS path of the Store appended with Auth

   $authentication = Add-STFAuthenticationService $authenticationVirtualPath
```

```
}

else

{

    Write-Output "An Authentication service already exists at the specified virtual path and will be used."

}
```

- Creates a new authentication service if one does not exist at the specified virtual path. The default authentication method of username and password is enabled.

```
# Determine if the authentication service at the specified virtual path exists

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

if(-not $authentication)

{

    # Add an Authentication service using the IIS path of the Store appended with Auth

    $authentication = Add-STFAuthenticationService $authenticationVirtualPath

}

else

{

    Write-Output "An Authentication service already exists at the specified virtual path and will be used."

}
```

- Creates the new store service configured with one XenDesktop controller with the servers defined in the array **$XenDesktopServers** at the specified virtual path if one does not already exist.

```
# Determine if the store service at the specified virtual path exists

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

if(-not $store)

{

# Add a Store that uses the new Authentication service configured to publish resources from the supplied servers

$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `

    -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

```
else
{
    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."
    # Get the number of farms configured in the store
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count
    # Append the farm to the store with a unique name
    Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port `
        -SSLRelayPort $SSLRelayPort -TransportType $TransportType
}
```

- Adds a Citrix Receiver for Web service at the specified IIS virtual path to access applications published in the store created above.

```
# Determine if the receiver service at the specified virtual path exists
$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath
if(-not $receiver)
{
    # Add a Receiver for Web site so users can access the applications and desktops in the published in the Store
    $receiver = Add-STFWebReceiverService -VirtualPath $receiverVirtualPath -StoreService $store
}
else
{
    Write-Output "A Web Receiver service already exists at the specified virtual path and will be used."
}
```

- Enables XenApp services for the store so older Citrix Receiver clients can connect to published applications.

```
# Determine if PNA is configured for the Store service
$storePnaSettings = Get-STFStorePna -StoreService $store
if(-not $storePnaSettings.PnaEnabled)
{
  # Enable XenApp services on the store and make it the default for this server
```



```
        Enable-STFStorePna -StoreService $store -AllowUserPasswordChange -DefaultPnaService
    }
```

Example: Create a remote access deployment

The following example builds on the previous script to add a deployment with remote access.

Before you begin, make sure you follow the steps detailed in Get Started with the SDK. This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and import the required StoreFront modules. Imports are not required in newer versions of PowerShell.

```
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
```

- Create an internal access StoreFront deployment by calling the previous examples script. The base deployment will be extended to support remote access.

```
# 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
```

- Gets services created in the simple deployment as they need to be updated to support the remote access scenario.

```
# 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
```

- Enables CitrixAGBasic on the Citrix Receiver for Web service required for remote access using NetScaler Gateway. Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols.

```
# 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
```

- Enables CitrixAGBasic on the authentication service. This is required for remote access.

```
# 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
```

- Adds a new remote access Gateway, adding the optional subnet ipaddress is supplied and registers it with the store to be accessed remotely.

```
# 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
```

Example: Create a remote access deployment with optimal launch Gateway

The following example builds on the previous script to add a deployment with optimal launch Gateway remote access.

Before you begin, make sure you follow the steps detailed in Get Started with the SDK. This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and imports the required StoreFront modules. Imports are not required in newer versions of PowerShell.

```
Param(
  [Parameter(Mandatory=$true)]
  [Uri]$HostbaseUrl,
  [long]$SiteId = 1,
  [string]$Farmtype = "XenDesktop",
  [Parameter(Mandatory=$true)]
  [string[]]$FarmServers,
  [string]$StoreVirtualPath = "/Citrix/Store",
  [bool]$LoadbalanceServers = $false,
  [int]$Port = 80,
  [int]$SSLRelayPort = 443,
  [ValidateSet("HTTP","HTTPS","SSL")]
  [string]$TransportType = "HTTP",
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayUrl,
  [Parameter(Mandatory=$true)]
  [Uri]$GatewayCallbackUrl,
  [Parameter(Mandatory=$true)]
```

```
    [string[]]$GatewaySTAUrls,

    [string]$GatewaySubnetIP,

    [Parameter(Mandatory=$true)]

    [string]$GatewayName,

    [Parameter(Mandatory=$true)]

    [Uri]$OptimalGatewayUrl,

    [Parameter(Mandatory=$true)]

    [string[]]$OptimalGatewaySTAUrls,

    [Parameter(Mandatory=$true)]

    [string]$OptimalGatewayName

)

Set-StrictMode -Version 2.0

# 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
```

- Calls into the remote access deployment script to configure the basic deployment and add remote access.

```
# Create a remote access deployment

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath
$StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType
$TransportType `

  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
GatewayName $GatewayName
```

- Adds the preferred optimal launch gateway and get it from the list of configured gateways.

  # Add a new Gateway used for remote HDX access to desktops and apps

  $gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru

- Gets the store service to use the optimal gateway, register it assigning it to launches from the farm named.

  # 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

Example: Create a deployment with a Desktop Appliance site

TThe following example builds on the simple deployment example to add a deployment with Desktop Appliance site.

Before you begin, make sure you follow the steps detailed in Get Started with the SDK. This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note: To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and import the required StoreFront modules. Imports are not required in newer versions of PowerShell.

  Param(

  [Parameter(Mandatory=$true)]

  [Uri]$HostbaseUrl,

  [long]$SiteId = 1,

  [string]$Farmtype = "XenDesktop",

  [Parameter(Mandatory=$true)]

  [string[]]$FarmServers,

  [string]$StoreVirtualPath = "/Citrix/Store",

  [bool]$LoadbalanceServers = $false,


```
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
# 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
```

- Automate a desktop appliance path based on that of the $StoreVirtualPath.

```
$desktopApplianceVirtualPath = "$($StoreIISPath.TrimEnd('/'))Appliance"
```

- Calls into the simple deployment script to configure a default deployment with the required services.

```
# Create a remote access deployment

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent

$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath
$StoreVirtualPath -Farmtype $Farmtype `

  -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType
$TransportType `

  -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
GatewayName $GatewayName
```

- Gets the store service to use for the Desktop Appliance site. Use the **Add-STFDesktopApplianceService** cmdlet to add the new site with MultiDesktop and Explicit username and password authentication.

```
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Create a new Desktop Appliance site using the desktops published by the Store Service

Add-STFDesktopApplianceService -VirtualPath $desktopApplianceVirtualPath -StoreService $store -EnableExplicit
```

Example: Exchange metadata between the Identity Provider and the Service Provider (StoreFront) for SAML authentication

SAML authentication can be configured in the StoreFront management console (see Configure the authentication service) or using the following PowerShell cmdlets: Export-STFSamlEncryptionCertificate, Export-STFSamlSigningCertificate, Import-STFSamlEncryptionCertificate, Import-STFSamlSigningCertificate, New-STFSamlEncryptionCertificate, New-STFSamlIdPCertificate, New-STFSamlSigningCertificate.

You can use the cmdlet, **Update-STFSamlIdPFromMetadata**, to exchange metadata (identifiers, certificates, endpoints and other configuration) between the Identity Provider and the Service Provider, which is StoreFront in this case.

For a StoreFront Store, named "Store", with its dedicated authentication service, the metadata endpoint will be:

https://<storefront host>/Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata

If your Identity Provider supports metadata import, then you can point it at the above URL. **Note**: This must be done over HTTPS.

For StoreFront to consume the metadata from an Identity Provider, the following PowerShell can be used:

```
command                                                                                    コピー
```



```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module



# Remember to change this with the virtual path of your Store.

$StoreVirtualPath = "/Citrix/Store"



$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store



# To read the metadata directly from the Identity Provider, use the following:

# Note again this is only allowed for https endpoints

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMeta



# If the metadata has already been download, use the following:

# Note: Ensure that the file is encoded as UTF-8

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata
```

Example: List the metadata and ACS endpoints for a specified store for SAML authentication

You can use the following script to list out the metadata and ACS (Assertion Consumer Service) endpoints for a specified store.

```
command
```
コピー

```
# 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"
```

Example of the output

```
command
```
コピー

```
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
```

Troubleshoot StoreFront

May 22, 2017

When StoreFront is installed or uninstalled, the following log files are created by the StoreFront installer in the C:\Windows\Temp\ directory. The file names reflect the components that created them and include time stamps.

- Citrix-DeliveryServicesRoleManager-*.log—Created when StoreFront is installed interactively.
- Citrix-DeliveryServicesSetupConsole-*.log—Created when StoreFront is installed silently and when StoreFront is uninstalled, either interactively or silently.
- CitrixMsi-CitrixStoreFront-x64-*.log—Created when StoreFront is installed and uninstalled, either interactively or silently.

StoreFront supports Windows event logging for the authentication service, stores, and Receiver for Web sites. Any events that are generated are written to the StoreFront application log, which can be viewed using Event Viewer under either Application and Services Logs > Citrix Delivery Services or Windows Logs > Application. You can control the number of duplicate log entries for a single event by editing the configuration files for the authentication service, stores, and Receiver for Web sites.

The Citrix StoreFront management console automatically records tracing information. By default, tracing for other operations is disabled and must be enabled manually. Logs created by Windows PowerShell commands are stored in the \Admin\logs\ directory of the StoreFront installation, typically located at C:\Program Files\Citrix\Receiver StoreFront\. The log file names contain command actions and subjects, along with time stamps that can be used to differentiate command sequences.

Important: In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group so that the other servers in the deployment are updated.

To configure log throttling

1. Use a text editor to open the web.config file for the authentication service, store, or Receiver for Web site, which are typically located in the C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\, and C:\inetpub\wwwroot\Citrix\storenameWeb\ directories, respectively, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.
   <logger duplicateInterval="00:01:00" duplicateLimit="10">
   By default, StoreFront is configured to limit the number of duplicate log entries to 10 per minute.
3. Change the value of the duplicateInterval attribute to the set the time period in hours, minutes, and seconds over which duplicate log entries are monitored. Use the duplicateLimit attribute to set the number of duplicate entries that must be logged within the specified time interval to trigger log throttling.

When log throttling is triggered, a warning message is logged to indicate that further identical log entries will be suppressed. Once the time limit elapses, normal logging resumes and an informational message is logged indicating that duplicate log entries are no longer being suppressed.

To enable tracing

Caution: The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of

the PowerShell before opening the StoreFront console.

1. Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, type the following commands and restart the server to enable tracing.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Verbose
   Allowed values for -TraceLevel are, in increasing levels of tracing detail: Off, Error, Warning, Info, Verbose.
   StoreFront automatically captures Error trace messages. Due to the large amount of data that can potentially be generated, tracing may significantly impact the performance of StoreFront, so it is recommended that the Info or Verbose levels are not used unless specifically required for troubleshooting.

   Optional arguments for the Set-DSTraceLevel cmdlet are:
   -FileCount: Specifies the number of trace files (default = 3)
   -FileSizeKb: Specifies the maximum size of each trace file (default = 1000)
   -ConfigFile <FileName>: An alternative to -All that allows a specific configuration file to be updated rather than all. For example, a -ConfigFile value of c:\inetpub\wwwroot\Citrix\<StoreName>\web.config would set tracing for the Store with the name <StoreName>.

2. To disable tracing, type the following commands and restart the server.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands

   Set-DSTraceLevel -All -TraceLevel Off

When tracing is enabled, tracing information is written in the \Admin\Trace\ directory of the StoreFront installation located at C:\Program Files\Citrix\Receiver StoreFront\.