StoreFront 3.12

Aug 14, 2017

Administración de un sitio de Citrix Receiver para Web

Configuración del acceso de usuarios

Configuración de la alta disponibilidad para las tiendas

Integración con NetScaler y NetScaler Gateway

Configuraciones avanzadas

Configuración mediante archivos de configuración

Acerca de StoreFront

Aug 14, 2017

StoreFront administra la entrega de escritorios y aplicaciones desde los servidores XenMobile, XenApp y XenDesktop del centro de datos a los dispositivos de los usuarios. StoreFront enumera y agrega las aplicaciones y los escritorios disponibles en tiendas. Los usuarios pueden acceder a las tiendas de StoreFront directamente desde Citrix Receiver o si navegan a un sitio de Desktop Appliance o de Citrix Receiver para Web. Los usuarios también pueden acceder a StoreFront mediante clientes ligeros y otros dispositivos finales compatibles a través de un sitio de servicios XenApp.

StoreFront mantiene un registro de las aplicaciones de cada usuario y actualiza automáticamente sus dispositivos. Los usuarios tienen una experiencia uniforme a medida que se mueven entre sus smartphones, tabletas, equipos portátiles y equipos de escritorio. StoreFront es el componente fundamental de XenApp 7.x y XenDesktop 7.x, aunque se puede utilizar con otras versiones de XenApp y XenDesktop.

Novedades en StoreFront

StoreFront 3.12 incluye una serie de problemas resueltos y conocidos.

Integración de las aplicaciones de Citrix Online en las tiendas. Hemos anunciado que esta característica quedará obsoleta en XenApp y XenDesktop 7.14 (StoreFront 3.11). En 3.12, esta función no puede configurarse en la consola de administración de StoreFront.Si actualiza a StoreFront 3.12, podrá seguir usando esta característica. Para cambiar la configuración, use el cmdlet de PowerShell llamado Update-DSGenericApplications. Para obtener más información, consulte Integración de las aplicaciones de Citrix Online en las tiendas.

Problemas resueltos

Aug 14, 2017

Se han solucionado los problemas siguientes desde la versión 13.11:

- Si el administrador modifica el parámetro MaxPasswordAge de la directiva de grupo, el servicio de dominio predeterminado de StoreFront no carga el nuevo valor. En StoreFront, el usuario puede ver "una cantidad incorrecta de días restantes hasta la caducidad de la contraseña".

  Nota: Este problema está resuelto. Sin embargo, el nuevo valor puede llegar a tardar una hora en cargarse.

  [#DNA-41380]

- Es posible que no pueda volver a conectarse a sesiones desconectadas en una implementación de agrupación multisitio. Por eso, puede recibir una segunda instancia del mismo recurso.

  [#LC7453]

- Cuando se inhabilita una fuente de una aplicación agregada, la aplicación puede ocultarse inesperadamente al usuario final.

  [#LC7675]

- En StoreFront, puede que no se inhabilite la opción de autoservicio de cuentas, incluso aunque la opción aparezca inhabilitada.

  [#LC7744]

- En StoreFront, si intenta quitar la autenticación compartida de tiendas, puede aparecer el siguiente mensaje de error al guardar los cambios:
  "Ocurrió un error al guardar los cambios".

  [#LC7781]

Problemas conocidos

Aug 14, 2017

Estos son los problemas conocidos de esta versión.

- El control del área de trabajo se vuelve a conectar a la sesión de una sola aplicación, en lugar de reconectarse a todas las aplicaciones del área de trabajo. Este problema se presenta cuando se utiliza Chrome para acceder el sitio de Receiver para Web. Para solucionar temporalmente este problema, haga clic en "Conectar" en cada aplicación desconectada.

  [# DNA-25140]

- Los usuarios no pueden iniciar sesión en Citrix Receiver para Web si un formulario de autenticación personalizado contiene un elemento con ID=confirmBtn. Como solución temporal, cambie el valor ID de la extensión de autenticación en el formulario personalizado.

  [# 603196, DNA-22593]

- La reconexión de aplicaciones en el explorador Chrome puede fallar. Si se reconecta a las aplicaciones publicadas cuando hay más de una sesión en uso, hacer clic en **Conectar** le reconectará a la primera sesión. Solución temporal: Haga clic en **Conectar** de nuevo para volver a conectar cada sesión adicional.

  [# 575364, DNA-22561]

Avisos de terceros

Aug 14, 2017

StoreFront pueden incluir software de terceros con licencias definidas en los términos del siguiente documento:

PDF Avisos de terceros para StoreFront

Requisitos del sistema

Aug 14, 2017

Al planificar la instalación, Citrix recomienda dejar al menos 2 GB de RAM adicionales para StoreFront por encima de los requisitos de otros productos instalados en el servidor. El servicio de suscripción de la tienda requiere un mínimo de 5 MB de espacio en disco, además de aproximadamente 8 MB por cada 1000 suscripciones a aplicaciones. Todas las demás especificaciones de hardware deben satisfacer los requisitos mínimos del sistema operativo instalado.

Después de las pruebas pertinentes, Citrix proporciona respaldo para las instalaciones de StoreFront en las siguientes plataformas:

- Windows Server 2016 ediciones Datacenter y Standard
- Windows Server 2012 R2 ediciones Datacenter y Standard
- Windows Server 2012 ediciones Datacenter y Standard
- Windows Server 2008 R2 Service Pack 1 ediciones Enterprise y Standard

La actualización de la versión de sistema operativo en un servidor que ejecuta StoreFront no está respaldada. Citrix recomienda instalar StoreFront en una instalación limpia del sistema operativo. En una implementación con varios servidores, todos los servidores deben ejecutar la misma versión del sistema operativo y la misma configuración regional. No se respaldan los grupos de servidores StoreFront que contengan combinaciones de versiones de sistema operativo y configuraciones regionales. Aunque un grupo de servidores puede contener hasta seis servidores como máximo, desde el punto de vista de la capacidad basada en simulaciones, no hay ventaja alguna en crear grupos que contengan más de tres servidores. Todos los servidores de un grupo deben residir en la misma ubicación.

Microsoft Internet Information Services (IIS) y Microsoft .NET Framework son necesarios en el servidor. Si algunos de estos requisitos previos están instalados, pero no habilitados, el instalador de StoreFront los habilita antes de instalar el producto. Antes de instalar StoreFront, debe instalar Windows PowerShell y Microsoft Management Console (ambos son componentes predeterminados de Windows Server) en el servidor Web. La ruta relativa a StoreFront en IIS debe ser la misma para todos los servidores de un grupo.

El instalador de StoreFront agregará las características de IIS necesarias. Si quiere instalar previamente estas características, esta es la lista:

En todas las plataformas:

- 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

En Windows Server 2008 R2:

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

En Windows Server 2012 R2:

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

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

StoreFront utiliza los siguientes puertos para las comunicaciones. Asegúrese de que los firewalls y otros dispositivos de red permitan el acceso a estos puertos.

- Los puertos TCP 80 y 443 se usan para comunicaciones HTTP y HTTPS respectivamente, y deben ser accesibles tanto desde dentro como desde fuera de la red corporativa.
- El puerto TCP 808 se usa para las comunicaciones entre los servidores StoreFront y debe ser accesible desde dentro de la red corporativa.
- Para las comunicaciones entre los servidores StoreFront en un grupo de servidores se usa un puerto TCP, seleccionado de forma aleatoria de entre todos los puertos no reservados. Al instalar StoreFront, se configura una regla del Firewall de Windows para habilitar el acceso al ejecutable de StoreFront. Sin embargo, puesto que el puerto se asigna de forma aleatoria, debe asegurarse de que los firewalls u otros dispositivos de la red interna no bloqueen el tráfico a ninguno de los puertos TCP que no estén asignados.
- Citrix Receiver para HTML5 utiliza el puerto TCP 8008, cuando está habilitado, para la comunicación de los usuarios locales de la red interna con los servidores que suministran sus escritorios y aplicaciones.

StoreFront admite tanto entornos de solo IPv6 como entornos de doble pila de IPv4/IPv6.

Requisitos de infraestructura

Después de las pruebas pertinentes, Citrix proporciona respaldo para StoreFront cuando se usa con las siguientes versiones de productos Citrix.

Requisitos del servidor Citrix

Las tiendas de StoreFront combinan escritorios y aplicaciones de los siguientes productos.

- XenApp y XenDesktop 7.15
- XenApp y XenDesktop 7.14
- XenApp y XenDesktop 7.13
- XenApp y XenDesktop 7.12
- XenApp y XenDesktop 7.11
- XenApp y XenDesktop 7.9
- XenApp y XenDesktop 7.8
- XenApp y XenDesktop 7.7
- XenApp y XenDesktop 7.6
- XenApp y XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7

- XenApp 6.5
- XenMobile 9.0 o App Controller 9.0

Requisitos de NetScaler Gateway

Se pueden usar las siguientes versiones de NetScaler Gateway para proporcionar acceso a StoreFront a los usuarios de redes públicas.

- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 Compilación 69.4 (el número de versión aparece en la parte superior de la utilidad de configuración)

Requisitos de Citrix Receiver para HTML5

Tenga en cuenta los siguientes requisitos adicionales si desea permitir que los usuarios accedan a escritorios y aplicaciones a través de Citrix Receiver para HTML5 ejecutado en los sitios de Receiver para Web.

Para las conexiones de red interna, Citrix Receiver para HTML5 permite el acceso a los escritorios y las aplicaciones proporcionados por los siguientes productos.

- XenApp y XenDesktop 7.15
- XenApp y XenDesktop 7.14
- XenApp y XenDesktop 7.13
- XenApp y XenDesktop 7.12
- XenApp y XenDesktop 7.11
- XenApp y XenDesktop 7.9
- XenApp y XenDesktop 7.8
- XenApp y XenDesktop 7.7
- XenApp y XenDesktop 7.6
- XenApp y XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5 Feature Pack 2
- XenApp 6.5 Feature Pack 1 para Windows Server 2008 R2 (requiere la revisión hotfix XA650R01W2K8R2X64051, que está disponible en http://support.citrix.com/article/CTX135757)

Para los usuarios remotos desde fuera de la red corporativa, Citrix Receiver para HTML5 permite el acceso a los escritorios y aplicaciones a través de las siguientes versiones de NetScaler Gateway.

- NetScaler Gateway 11.*x*
- NetScaler Gateway 10.1
- Access Gateway 10 Compilación 71.6014 (el número de versión aparece en la parte superior de la utilidad de configuración)

En el caso de usuarios que se conectan a través de NetScaler Gateway, Citrix Receiver para HTML5 permite el acceso a los escritorios y las aplicaciones proporcionados por los siguientes productos.

- XenApp y XenDesktop 7.15

- XenApp y XenDesktop 7.14
- XenApp y XenDesktop 7.13
- XenApp y XenDesktop 7.12
- XenApp y XenDesktop 7.11
- XenApp y XenDesktop 7.9
- XenApp y XenDesktop 7.8
- XenApp y XenDesktop 7.7
- XenApp y XenDesktop 7.6
- XenApp y XenDesktop 7.5
- XenDesktop 7.1
- XenDesktop 7
- XenApp 6.5

Requisitos del dispositivo del usuario

StoreFront proporciona un amplio abanico de opciones para el acceso de los usuarios a escritorios y aplicaciones. Los usuarios de Citrix Receiver pueden acceder a las tiendas a través de Citrix Receiver, o pueden utilizar un explorador Web para iniciar sesión en el sitio de Citrix Receiver para Web de la tienda. Para los usuarios que no pueden instalar Citrix Receiver, pero tienen un explorador Web compatible con HTML5, puede proporcionar acceso a los escritorios y aplicaciones directamente desde el explorador Web mediante la habilitación de Citrix Receiver para HTML5 en los sitios de Citrix Receiver para Web.

Los usuarios con dispositivos de escritorio que no están unidos a ningún dominio acceden a los escritorios a través de sus exploradores Web, que se han configurado para tener acceso a los sitios de Desktop Appliance. En el caso de dispositivos de escritorio que no están unidos a ningún dominio y equipos reasignados que ejecutan Citrix Desktop Lock, junto con clientes Citrix anteriores que no se pueden actualizar, los usuarios deben conectarse a través de la URL de servicios XenApp para la tienda.

Si desea entregar aplicaciones sin conexión a los usuarios, se requiere el Offline Plug-in, además de Citrix Receiver para Windows. Si desea entregar a los usuarios secuencias de Microsoft Application Virtualization (App-V), también se requiere una versión compatible de Microsoft Application Virtualization Desktop Client. Para obtener más información, consulte el artículo Administración de aplicaciones distribuidas por streaming. Los usuarios no pueden acceder a aplicaciones sin conexión o a secuencias de App-V a través de sitios de Citrix Receiver para Web.

Se considera que todos los dispositivos de usuario cumplen los requisitos mínimos de hardware para el sistema operativo instalado.

Requisitos para tiendas con Citrix Receiver habilitado

Se pueden usar las siguientes versiones de Citrix Receiver para acceder a las tiendas de StoreFront mediante conexiones desde la red interna y a través de NetScaler Gateway. Es posible establecer conexiones a través de NetScaler Gateway mediante NetScaler Gateway Plug-in y/o el acceso sin cliente. Citrix Receiver para Windows 4.3 es la versión mínima necesaria para recibir la experiencia unificada completa de Citrix Receiver de StoreFront. Consulte Respaldo para la experiencia unificada de Citrix Receiver.

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

Requisitos para el acceso a las tiendas a través de sitios de Citrix Receiver para Web

Se recomiendan las siguientes combinaciones de Citrix Receiver, sistemas operativos y exploradores Web para el acceso de los usuarios a los sitios de Citrix Receiver para Web tanto a través de conexiones desde la red local como a través de NetScaler Gateway. Es posible establecer conexiones a través de NetScaler Gateway mediante NetScaler Gateway Plug-in y el acceso sin cliente.

- • De Citrix Receiver para Windows 4.2.x y versiones posteriores a Citrix Receiver para Windows 4.9
  - Windows 10 (ediciones de 32 y 64 bits)
    - Microsoft Edge
    - Internet Explorer 11
    - Google Chrome
    - Mozilla Firefox
  - Windows 8.1 (ediciones de 32 y 64 bits)
    - Internet Explorer 11 (modo de 32 bits)
    - Google Chrome
    - Mozilla Firefox
  - Windows 8 (ediciones de 32 y 64 bits)
    - Internet Explorer 10 (modo de 32 bits)
    - Google Chrome
    - Mozilla Firefox
  - Windows 7 Service Pack 1 (ediciones de 32 y 64 bits)
    - Internet Explorer 11, 10, 9
    - Google Chrome
    - Mozilla Firefox
  - Windows Embedded Standard 7 Service Pack 1 o Windows Thin PC
    - Internet Explorer 11, 10, 9
- Citrix Receiver para Windows 4.0 y Citrix Receiver para Windows 3.4
  - Windows 8 (ediciones de 32 y 64 bits)
    - Internet Explorer 10 (modo de 32 bits)
    - Google Chrome
    - Mozilla Firefox
  - Windows 7 Service Pack 1 (ediciones de 32 y 64 bits)
    - Internet Explorer 11, 10, 9
    - Google Chrome
    - Mozilla Firefox
  - Windows Embedded Standard 7 Service Pack 1 y Windows Thin PC
    - Internet Explorer 11, 10, 9
- Citrix Receiver para 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 para Linux 12.1 y Citrix Receiver para Linux 13.x
  - Ubuntu 12.04 (de 32 bits) y 14.04 LTS (de 32 bits)
    - Google Chrome
    - Mozilla Firefox

Requisitos para el acceso a escritorios y aplicaciones a través de Receiver para HTML5

Se recomiendan los siguientes sistemas operativos y exploradores Web para el acceso de los usuarios a escritorios y aplicaciones a través de Receiver para HTML5 ejecutado en los sitios de Receiver para Web. Se admiten tanto las conexiones de la red interna como las conexiones a través de NetScaler Gateway. Sin embargo, si se trata de conexiones desde la red interna, Receiver para HTML5 solo permite el acceso a los recursos proporcionados por productos específicos. Además, se necesitan versiones específicas de NetScaler Gateway para habilitar las conexiones desde fuera de la red corporativa. Para obtener más información, consulte Requisitos de infraestructura.

- Exploradores Web
  - Microsoft Edge
  - Internet Explorer 11 y 10 (solo conexiones HTTP)
  - Safari 7
  - Safari 6
  - Google Chrome
  - Mozilla Firefox
- Sistemas operativos
  - Windows RT
  - Windows 10 (ediciones de 32 y 64 bits)
  - Windows 8.1 (ediciones de 32 y 64 bits)
  - Windows 8 (ediciones de 32 y 64 bits)
  - Windows 7 Service Pack 1 (ediciones de 32 y 64 bits)
  - Windows Vista Service Pack 2 (ediciones de 32 y 64 bits)
  - Windows XP Embedded
  - 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 bits)

Requisitos para el acceso a las tiendas a través de sitios de Desktop Appliance

Se recomiendan las siguientes combinaciones de Citrix Receiver, sistema operativo y explorador Web para el acceso de los

usuarios a los sitios de Desktop Appliance desde la red interna. No se respaldan las conexiones a través de NetScaler Gateway.

- Citrix Receiver para Windows 4.5, Citrix Receiver para Windows 4.4, Citrix Receiver para Windows 4.3, Citrix Receiver para Windows 4.2.x y Citrix Receiver para Windows 4.1
  - Windows 8.1 (ediciones de 32 y 64 bits)
    - Internet Explorer 11 (modo de 32 bits)
  - Windows 8 (ediciones de 32 y 64 bits)
    - Internet Explorer 10 (modo de 32 bits)
  - Windows 7 Service Pack 1 (ediciones de 32 y 64 bits), Windows Embedded Standard 7 Service Pack 1 o Windows Thin PC
    - Internet Explorer 9 (modo de 32 bits)
    - Internet Explorer 8 (modo de 32 bits)
  - Windows XP Embedded
    - Internet Explorer 8 (modo de 32 bits)
- Citrix Receiver para Windows 4.0 o Citrix Receiver para Windows 3.4
  - Windows 8 (ediciones de 32 y 64 bits)
    - Internet Explorer 10 (modo de 32 bits)
  - Windows 7 Service Pack 1 (ediciones de 32 y 64 bits), Windows Embedded Standard 7 Service Pack 1 o Windows Thin PC
    - Internet Explorer 9 (modo de 32 bits)
    - Internet Explorer 8 (modo de 32 bits)
  - Windows XP Embedded
    - Internet Explorer 8 (modo de 32 bits)
- Citrix Receiver para Windows Enterprise 3.4
  - Windows 7 Service Pack 1 (ediciones de 32 y 64 bits), Windows Embedded Standard 7 Service Pack 1 o Windows Thin PC
    - Internet Explorer 9 (modo de 32 bits)
    - Internet Explorer 8 (modo de 32 bits)
  - Windows XP Embedded
    - Internet Explorer 8 (modo de 32 bits)
- Citrix Receiver para Linux 12.1
  - Ubuntu 12.04 (32 bits)
    - Mozilla Firefox 27

Requisitos para el acceso a las tiendas a través de las direcciones URL de servicios XenApp

Todas las versiones de Citrix Receiver enumeradas anteriormente se pueden usar para acceder a las tiendas de StoreFront con funcionalidad reducida a través de direcciones URL de servicios XenApp. Además, puede usar la versión antigua del cliente que no respalda otros métodos de acceso (Citrix Receiver para Linux 12.0, solo conexiones de red interna) para acceder a las tiendas a través de las direcciones URL de servicios XenApp. En caso de respaldo disponible, es posible establecer conexiones a través de NetScaler Gateway mediante NetScaler Gateway Plug-in y el acceso sin cliente.

Requisitos de tarjetas inteligentes

Requisito para usar Citrix Receiver para Windows 4.x con tarjetas inteligentes

Citrix hace pruebas de compatibilidad con tarjetas Common Access Card (CAC) del departamento de Defensa del Gobierno de los Estados Unidos, NIST PIV (Personal Identity Verification) del National Institute of Standards and Technology de Estados Unidos y con tokens de tarjeta inteligente USB. Puede usar los lectores de tarjeta con contacto que cumplen la especificación de los dispositivos de interfaz de tarjeta inteligente / de chip USB (CCID), que Zentraler Kreditausschuss (ZKA) clasifica como lectores de tarjetas inteligentes de Clase 1. Los lectores de tarjeta con contacto de Clase 1 de ZKA requieren que los usuarios inserten sus tarjetas inteligentes en el lector. No se admiten otros tipos de lectores de tarjetas inteligentes, incluidos los lectores de Clase 2 (que tienen teclados numéricos para escribir los PIN), los lectores de tarjetas sin contacto y las tarjetas inteligentes virtuales basadas en chips del Módulo de plataforma segura (TPM).

Para los dispositivos Windows, el respaldo para tarjeta inteligente se basa en las especificaciones estándar PC/SC de Microsoft. Como requisito mínimo, las tarjetas inteligentes y los lectores de tarjetas deben ser admitidos por el sistema operativo y haber recibido la Certificación de hardware en Windows.

Para obtener más información acerca de tarjetas inteligentes y middleware compatibles con Citrix, consulte Tarjetas inteligentes en la documentación de XenApp y XenDesktop, y http://www.citrix.com/ready.

Requisitos para usar sitios de Desktop Appliance con tarjetas inteligentes

En el caso de los usuarios con dispositivos de escritorio y PC reasignados que ejecutan Citrix Desktop Lock, se necesita Citrix Receiver para Windows Enterprise 3.4 para poder usar autenticación con tarjetas inteligentes. En todos los demás dispositivos de Windows, se puede usar Citrix Receiver para Windows 4.1.

Requisitos para la autenticación a través de NetScaler Gateway

Se pueden usar las siguientes versiones de NetScaler Gateway para proporcionar acceso a StoreFront si se trata de usuarios de redes públicas que se autentican con tarjetas inteligentes.

- NetScaler Gateway 11.x
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10 Compilación 69.4 (el número de versión aparece en la parte superior de la utilidad de configuración)

Planificación de una implementación de StoreFront

Aug 14, 2017

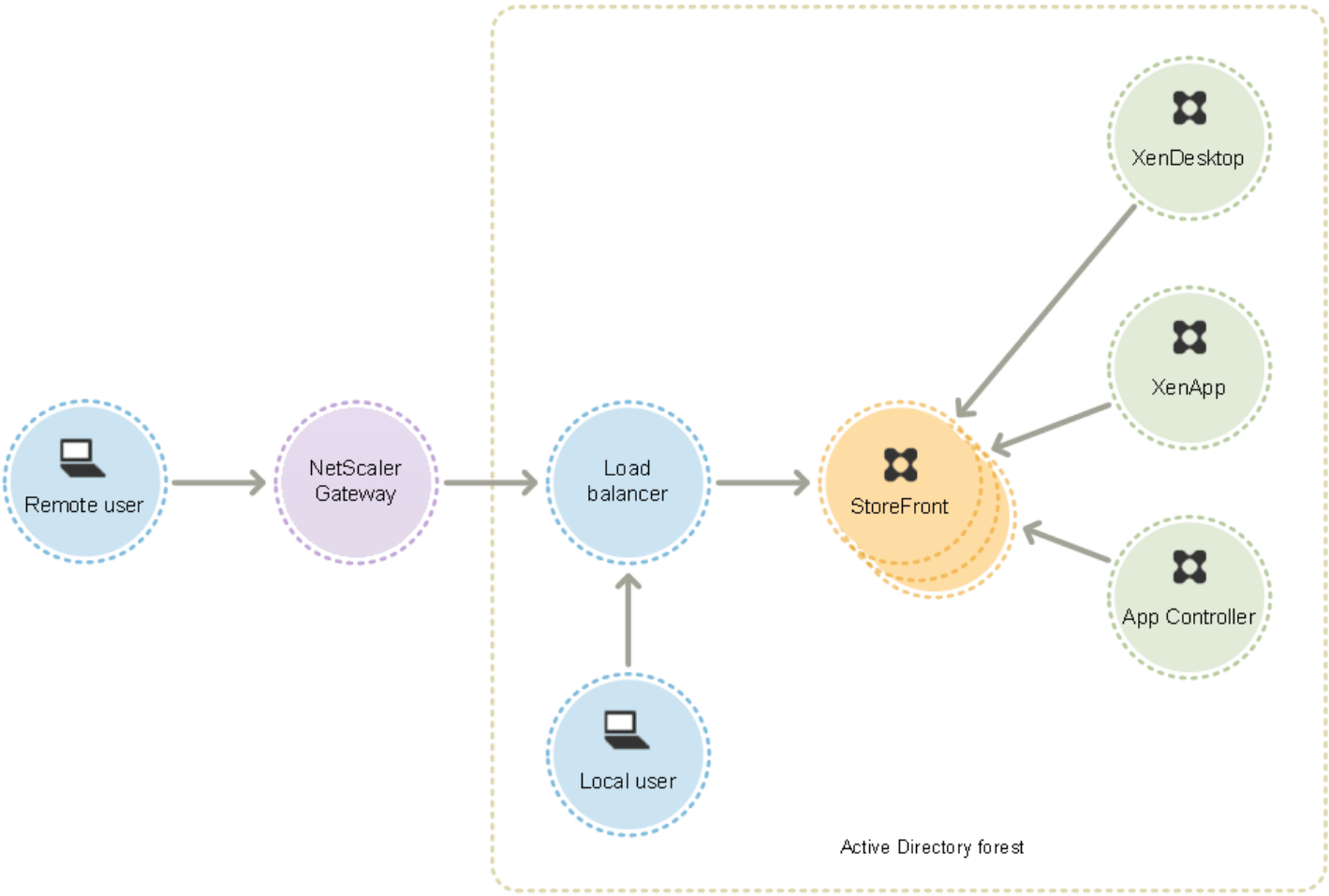
StoreFront utiliza la tecnología Microsoft .NET que se ejecuta en Microsoft Internet Information Services (IIS) para proporcionar las tiendas de aplicaciones de empresa que combinan recursos y ponerlos a disposición de los usuarios. StoreFront se integra con las implementaciones de XenDesktop, XenApp y App Controller para proporcionar a los usuarios un único punto de acceso de autoservicio a sus escritorios y aplicaciones.

StoreFront incluye los siguientes componentes principales:

- El servicio de autenticación autentica a los usuarios para Microsoft Active Directory, garantizando que esos usuarios no necesiten iniciar sesión de nuevo para acceder a sus escritorios y aplicaciones. Para obtener más información, consulte Autenticación de usuarios.
- Las tiendas enumeran y agregan escritorios y aplicaciones desde XenDesktop, XenApp y App Controller. Los usuarios acceden a las tiendas a través de Citrix Receiver, sitios de Citrix Receiver para Web, sitios de Desktop Appliance y direcciones URL de servicios XenApp. Para obtener más información, consulte Opciones de acceso de usuarios.
- El servicio de tiendas de suscripción registra información de las suscripciones a aplicaciones de los usuarios y actualiza sus dispositivos para garantizar una buena experiencia de usuario a los usuarios móviles. Para obtener más información acerca de maneras de mejorar la experiencia de los usuarios, consulte Mejora de la experiencia de usuario.

Es posible configurar StoreFront en un solo servidor o como una implementación con varios servidores. Las implementaciones con varios servidores no solo proporcionan capacidad adicional, sino que incrementan la disponibilidad. La arquitectura modular de StoreFront garantiza que la información acerca de la configuración y las suscripciones de los usuarios a las aplicaciones se almacena y se sincroniza entre todos los servidores de un grupo de servidores. Esto significa que si un servidor StoreFront deja de estar disponible por alguna razón, los usuarios pueden seguir accediendo a sus tiendas usando los demás servidores. Entretanto, los datos de configuración y suscripciones existentes en el servidor fallido se actualizan cuando dicho servidor se reconecta con su grupo de servidores. Los datos de suscripción se actualizan cuando se reanuda la conexión del servidor, pero debe propagar los cambios de la configuración si alguno se ha perdido mientras el servidor estaba sin conexión. En el caso de producirse un fallo de hardware que requiera la sustitución del servidor, puede instalar StoreFront en un nuevo servidor y agregarlo al grupo de servidores existente. El nuevo servidor se configurará y actualizará automáticamente con las suscripciones de los usuarios a las aplicaciones cuando se incorpore al grupo de servidores.

La figura muestra una implementación típica de StoreFront.



Equilibrio de carga

Para las implementaciones con varios servidores, se necesita equilibrio de carga externo a través de, por ejemplo, NetScaler o el equilibrio de carga de red de Windows. Configure el entorno de equilibrio de carga para la conmutación por error entre los servidores y así poder proporcionar una implementación con tolerancia de fallos. Para obtener más información acerca del equilibrio de carga con NetScaler, consulte Equilibrio de carga. Para obtener más información acerca del Equilibrio de carga de red de Windows, consulte http://technet.microsoft.com/en-us/library/hh831698.aspx.

Se recomienda activar el equilibrio de carga de las solicitudes enviadas desde StoreFront a los sitios de XenDesktop y las comunidades de XenApp en implementaciones con miles de usuarios, o cuando se registran cargas elevadas, por ejemplo cuando una gran cantidad de usuarios inician sesiones en un periodo breve de tiempo. Use un equilibrador de carga con monitores XML integrados y persistencia de sesiones, como NetScaler.

Si implementa un equilibrador de carga de terminación SSL o si necesita solucionar problemas, puede usar el cmdlet de PowerShell **Set-STFWebReceiverCommunication**.

Sintaxis:

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

Los valores válidos son:

- **On:** Este es el valor predeterminado para los sitios nuevos de Citrix Receiver para Web. Citrix Receiver para Web usa el

esquema (HTTPS o HTTP) y el número de puerto de la URL base, pero sustituye el host por la dirección IP de bucle para comunicar con los servicios de StoreFront. Esto funciona para implementaciones de servidor único y para implementaciones que tienen un equilibrador de carga sin terminación SSL.

- **OnUsingHttp:** Citrix Receiver para Web usa HTTP y la dirección IP de bucle para comunicarse con los servicios de StoreFront. Si está usando un equilibrador de carga con terminación SSL, seleccione este valor. También debe especificar el puerto HTTP si éste no es el predeterminado (80).
- **Off:** Este valor desactiva el bucle y Citrix Receiver para Web usa la URL base de StoreFront para comunicarse con los servicios de StoreFront. Si realiza una actualización en contexto, éste es el valor predeterminado para evitar la interrupción de la implementación existente.

Por ejemplo, si va a usar un equilibrador de carga con terminación SSL, su IIS está configurado para usar el puerto 81 para HTTP y la ruta al sitio de Citrix Receiver para Web es /Citrix/StoreWeb, puede ejecutar el comando siguiente para configurar el sitio de Citrix Receiver para Web:

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

Tenga en cuenta que tiene que desactivar el bucle invertido para usar cualquier herramienta de proxy Web, como Fiddler, para capturar el tráfico de red entre Citrix Receiver para Web y los servicios de StoreFront.

Consideraciones sobre Active Directory

En el caso de implementaciones de servidor único, StoreFront puede instalarse en un servidor que no esté unido a un dominio (aunque ciertas funciones no estarán disponibles). Los servidores StoreFront deben residir ya sea en el dominio de Active Directory que contiene las cuentas de los usuarios, o en un dominio que tenga una relación de confianza con el dominio de las cuentas de usuario, a menos que se habilite la delegación de la autenticación en las comunidades o sitios de XenApp y XenDesktop. Todos los servidores StoreFront pertenecientes a un grupo deben residir en el mismo dominio.

Conexiones de usuario

En un entorno de producción, Citrix recomienda utilizar HTTPS para proteger la comunicación entre los dispositivos de los usuarios y StoreFront. Para utilizar HTTPS, StoreFront requiere que la instancia de IIS que aloja el servicio de autenticación y las tiendas asociadas esté configurada para HTTPS. Sin una configuración de IIS adecuada, StoreFront utiliza HTTP para las comunicaciones. Puede cambiar de HTTP a HTTPS en cualquier momento que desee, siempre que tenga la configuración de IIS apropiada.

Si desea habilitar el acceso a StoreFront desde fuera de la red corporativa, se necesita NetScaler Gateway para proteger las conexiones de los usuarios remotos. Implemente NetScaler Gateway fuera de la red corporativa, con firewalls que separen NetScaler Gateway de redes tanto públicas como internas. Asegúrese de que NetScaler Gateway puede acceder al bosque de Active Directory que contiene los servidores StoreFront.

Varios sitios Web de Internet Information Services (IIS)

StoreFront le permite implementar distintas tiendas de aplicaciones en sitios Web de IIS diferentes en cada servidor Windows, de forma que cada tienda tenga un nombre de host y un enlace de certificado diferentes.

Empiece creando dos sitios Web, además del sitio Web predeterminado de IIS. Después de crear varios sitios Web en IIS, use el SDK de PowerShell para crear una implementación de StoreFront en cada uno de ellos. Para obtener más información sobre cómo crear sitios Web en IIS, consulte How to set up your first IIS Website.

Nota: Las consolas de StoreFront y PowerShell no pueden estar abiertas al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.

Ejemplo: Creación de dos implementaciones en sitios Web de IIS, una para aplicaciones y otra para escritorio.

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

StoreFront inhabilita la consola de administración cuando detecta varios sitios y muestra un mensaje a tal efecto.

Para obtener más información, consulte Antes de la Instalación y la configuración.

Escalabilidad

La cantidad de usuarios de Citrix Receiver que puede aceptar un único grupo de servidores StoreFront depende del hardware que utilice y del nivel de actividad de los usuarios. Basándose en una simulación de actividad donde los usuarios inician sesiones, enumeran 100 aplicaciones publicadas e inician un recurso, necesitará un servidor StoreFront con unas especificaciones mínimas recomendadas de dos CPU virtuales ejecutadas sobre un procesador dual Intel Xeon L5520 2.27Ghz de servidor, para acomodar hasta 30 000 conexiones de usuario por hora.

Necesitará un grupo de servidores con dos servidores configurados de la misma forma para acomodar hasta 60 000 conexiones de usuario por hora; tres nodos para 90 000 conexiones por hora, cuatro nodos para 120 000 conexiones por hora, 5 nodos para 150 000 conexiones por hora, y 6 nodos para 175 000 conexiones por hora.

El rendimiento de un único servidor StoreFront también se puede incrementar asignando más CPU virtuales al sistema. Cuatro CPU virtuales permiten 55 000 conexiones de usuario por hora y 8 CPU virtuales permitan hasta 80 000 conexiones por hora.

La asignación mínima de memoria recomendada para cada servidor es de 4 GB. Si usa Citrix Receiver para Web, asigne 700 bytes adicionales por recurso y por usuario además de la asignación básica de memoria.Al igual que cuando se usa Receiver para Web, al usar Citrix Receiver, diseñe su entorno para acomodar 700 bytes adicionales por cada recurso y por cada usuario, además de los requisitos básicos de 4 GB de memoria para esta versión de StoreFront.

Los patrones de uso de su entorno serán probablemente distintos de los descritos en las simulaciones mencionadas, por lo que sus servidores podrían admitir una cantidad mayor o menor de conexiones de usuario por hora.

Importante: Todos los servidores de un grupo deben residir en la misma ubicación. No se respaldan los grupos de servidores StoreFront que contengan combinaciones de versiones de sistema operativo y configuraciones regionales.

Consideraciones acerca del tiempo de espera

En ocasiones, pueden darse problemas de red o de otra índole entre una tienda de StoreFront y el servidor con el que se comunica, lo que provoca retrasos o fallos para los usuarios. Puede recurrir al parámetro de tiempo de espera de las tiendas para reajustar este comportamiento. Si especifica un valor bajo de tiempo de espera, StoreFront abandona rápidamente el servidor que falle y prueba otro. Esto es útil si, por ejemplo, ha configurado varios servidores para el proceso de conmutación por error.

Si especifica un tiempo de espera más elevado, StoreFront espera más para obtener una respuesta de los servidores. Esto es muy útil en entornos donde la fiabilidad de la red o de los servidores no es plena y suelen producirse retrasos.

Citrix Receiver para Web también tiene un parámetro de tiempo de espera, que controla por cuánto tiempo un sitio de Citrix Receiver para Web espera, para obtener una respuesta desde una tienda. Establezca un valor para este parámetro de

tiempo de espera que, al menos, equivalga al tiempo de espera de la tienda. Un tiempo de espera más elevado equivale a una mayor tolerancia de fallos, pero los usuarios pueden sufrir retrasos largos. Un tiempo de espera más bajo reduce las de los usuarios, pero es posible que experimenten más errores.

Para obtener información sobre la configuración de tiempo de espera, consulte Duración del tiempo de espera de las comunicaciones y de los reintentos en el servidor y Duración del tiempo de espera y reintentos de las comunicaciones.

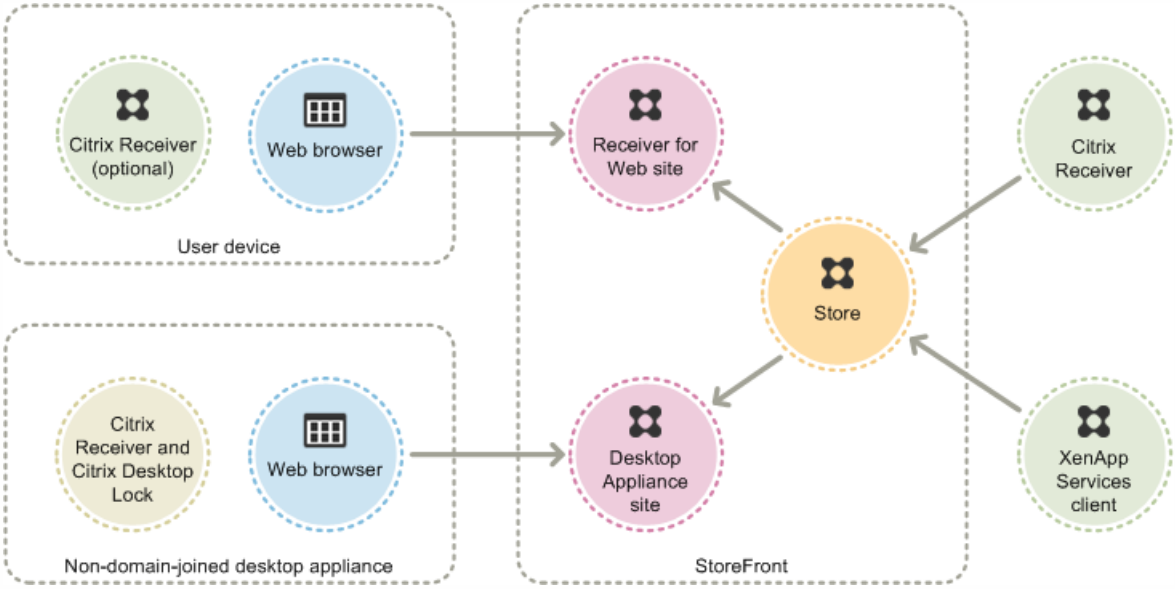
Opciones de acceso de usuarios

Aug 14, 2017

Los usuarios pueden acceder a las tiendas de StoreFront mediante cuatro métodos distintos.

- Citrix Receiver: Los usuarios con versiones compatibles de Citrix Receiver pueden acceder a las tiendas de StoreFront desde la interfaz de usuario de Citrix Receiver. El acceso a las tiendas desde Citrix Receiver ofrece la mejor experiencia de usuario y la máxima funcionalidad.
- Sitios de Receiver para Web: Los usuarios con exploradores Web compatibles pueden acceder a las tiendas de StoreFront navegando a los sitios de Citrix Receiver para Web. De forma predeterminada, los usuarios también deben tener una versión compatible de Citrix Receiver para acceder a los escritorios y aplicaciones. Sin embargo, puede configurar los sitios de Citrix Receiver para Web para permitir que los usuarios con exploradores Web compatibles con HTML5 puedan acceder a sus recursos sin instalar Citrix Receiver. Al crear una nueva tienda, se crea un sitio de Citrix Receiver para Web de forma predeterminada para la tienda.
- Sitios de Desktop Appliance: Los usuarios con dispositivos de escritorio no unidos a ningún dominio pueden acceder a los escritorios a través de los exploradores Web de sus dispositivos, que se han configurado para tener acceso a los sitios de Desktop Appliance en modo de pantalla completa. Cuando se crea una tienda para una implementación de XenDesktop mediante Citrix Studio, también se crea de forma predeterminada un sitio de Desktop Appliance para la tienda.
- Direcciones URL de servicios XenApp: Los usuarios de dispositivos de escritorio unidos a un dominio y PC reasignados que ejecuten el Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a las tiendas mediante la URL de servicios XenApp para la tienda. Al crear una nueva tienda, la URL de servicios XenApp correspondiente se habilita de forma predeterminada.

La ilustración muestra las opciones de acceso a las tiendas de StoreFront:



Citrix Receiver

El acceso a las tiendas desde dentro de la interfaz de usuario de Citrix Receiver ofrece la mejor experiencia de usuario y la mayor funcionalidad. Para ver las versiones de Citrix Receiver que pueden usarse para acceder a las tiendas de esta manera, consulte Requisitos del sistema.

Citrix Receiver utiliza direcciones URL internas y externas como balizas. Al intentar ponerse en contacto con estas balizas, Citrix Receiver puede determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un

escritorio o aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan devolver a Citrix Receiver los correspondientes datos de conexión. Esto permite a Citrix Receiver asegurarse de que no se solicitará a los usuarios que inicien sesión de nuevo cuando accedan a un escritorio o aplicación. Para obtener más información, consulte Configuración de balizas.

Después de la instalación, Citrix Receiver debe configurarse con los datos de conexión de las tiendas que suministran aplicaciones y escritorios de usuario. Si quiere facilitar el proceso de configuración para los usuarios, proporcióneles la información necesaria de una de las siguientes formas.

Importante: De forma predeterminada, Citrix Receiver requiere conexiones HTTPS para las tiendas. Si StoreFront no está configurado para HTTPS, los usuarios deben llevar a cabo pasos de configuración adicionales para usar conexiones HTTP. Citrix recomienda encarecidamente no habilitar conexiones de usuario no seguras a StoreFront en un entorno de producción. Para obtener más información, consulte *Configuración e instalación de Citrix Receiver para Windows mediante parámetros de línea de comandos* en la documentación de Citrix Receiver para Windows.

Archivos de aprovisionamiento

Es posible proporcionar a los usuarios archivos de aprovisionamiento que contengan los datos de conexión a sus tiendas. Después de instalar Citrix Receiver, los usuarios pueden abrir el archivo .cr para configurar automáticamente las cuentas para las tiendas. De forma predeterminada, los sitios de Citrix Receiver para Web ofrecen a los usuarios un archivo de aprovisionamiento para la única tienda para la que esté configurado el sitio en cuestión. Puede indicar a los usuarios que visiten los sitios de Receiver para Web de las tiendas a las que deseen tener acceso y descarguen los archivos de aprovisionamiento desde esos sitios. De forma alternativa, para un mayor control, puede usar la consola de administración de Citrix StoreFront para generar archivos de aprovisionamiento que contengan los datos de conexión para una o más tiendas. A continuación, puede distribuir estos archivos a los usuarios adecuados. Para obtener más información, consulte Exportación de archivos de aprovisionamiento de tiendas para los usuarios.

Direcciones URL de configuración generadas automáticamente

Para los usuarios que ejecutan sistemas operativos Mac, es posible utilizar Setup URL Generator de Citrix Receiver para Mac con el fin de crear una URL que contenga los datos de conexión de una tienda. Después de instalar Citrix Receiver, los usuarios pueden hacer clic en la URL para configurar automáticamente una cuenta para la tienda. Introduzca información de su implementación en la herramienta y genere una URL que se pueda distribuir automáticamente a los usuarios.

Configuración manual

Los usuarios más avanzados pueden crear nuevas cuentas introduciendo direcciones URL de tiendas en Citrix Receiver. Los usuarios remotos que acceden a StoreFront a través de NetScaler Gateway 10.1 y Access Gateway 10 introducen la dirección URL del dispositivo. Citrix Receiver obtiene la información necesaria para la configuración de la cuenta cuando se establece una conexión por primera vez. Si los usuarios se conectan a través de Access Gateway 9.3, no podrán configurar cuentas manualmente y deberán usar alguno de los métodos alternativos descritos anteriormente. Para obtener más información, consulte la documentación de Citrix Receiver.

Detección de cuentas basada en direcciones de correo electrónico

Los usuarios que instalen por primera vez Citrix Receiver en un dispositivo pueden configurar cuentas con sus direcciones de correo electrónico si descargan Citrix Receiver del sitio Web de Citrix o de una página de descarga de Citrix Receiver alojada en la red interna. Puede configurar los registros SRV de los recursos del localizador de NetScaler Gateway o StoreFront en su servidor DNS de Active Directory de Microsoft. Los usuarios no necesitan conocer la información de acceso a las tiendas,

simplemente deben introducir sus direcciones de correo electrónico durante la configuración inicial de Citrix Receiver. Citrix Receiver se comunica con el servidor DNS del dominio especificado en la dirección de correo electrónico y obtiene la información agregada al registro SRV de recursos. Posteriormente, se muestra una lista de las tiendas a las que los usuarios pueden acceder mediante Citrix Receiver.

Configuración de la detección de cuentas basada en direcciones de correo electrónico

Configure la detección de cuentas basada en direcciones de correo electrónico para que los usuarios que instalan Citrix Receiver por primera vez en un dispositivo puedan configurar sus cuentas con sus direcciones de correo electrónico. Dado que descargan Citrix Receiver del sitio Web de Citrix o una página de descarga de Citrix Receiver alojada en la red interna, los usuarios no necesitan saber los datos de acceso a las tiendas cuando instalan y configuran Citrix Receiver. La detección de cuentas basada en direcciones de correo electrónico está disponible si Citrix Receiver se descarga desde cualquier otra ubicación, como un sitio de Receiver para Web. Tenga en cuenta que ReceiverWeb.exe o ReceiverWeb.dmg descargados desde Citrix Receiver para Web no piden a los usuarios que configuren una tienda. Los usuarios aún pueden utilizar la opción Agregar cuenta e introducir su correo electrónico.

Durante el proceso de configuración inicial, Citrix Receiver pide a los usuarios que introduzcan una dirección de correo electrónico o una URL de tienda. Cuando un usuario introduce una dirección de correo electrónico, Citrix Receiver se comunica con el servidor DNS de Microsoft Active Directory según el dominio especificado en la dirección de correo electrónico para obtener una lista de tiendas disponibles en la que el usuario pueda seleccionarlas.

Para permitir que Citrix Receiver busque las tiendas disponibles en función de las direcciones de correo electrónico de los usuarios, configure los registros SRV de los recursos del localizador para NetScaler Gateway o StoreFront en el servidor DNS. Como recurso en caso de que no funcione, también puede implementar StoreFront en un servidor llamado "discoverReceiver.domain", donde domain es el dominio que contiene las cuentas de correo electrónico de los usuarios. Si no se encuentra ningún registro SRV en el dominio especificado, Citrix Receiver busca una máquina denominada "discoverReceiver" para identificar un servidor StoreFront.

Para permitir la detección de cuentas basada en direcciones de correo electrónico, es necesario instalar un certificado de servidor válido en el dispositivo NetScaler Gateway o en el servidor StoreFront. También es necesario que la cadena completa al certificado raíz sea válida. Para una experiencia de usuario óptima, instale un certificado con una entrada de Sujeto o Nombre alternativo del sujeto con el valor discoverReceiver.domain, donde domain es el dominio que contiene las cuentas de correo electrónico de los usuarios. Aunque se puede usar un certificado comodín para el dominio que contiene las cuentas de correo electrónico de los usuarios, primero es necesario asegurarse de que la implementación de dichos certificados está permitida por las directivas de seguridad de la empresa. También se pueden usar otros certificados para el dominio de las cuentas de correo electrónico de los usuarios, pero los usuarios verán un cuadro de diálogo de advertencia acerca de los certificados cuando Citrix Receiver se conecte por primera vez al servidor StoreFront. La detección de cuentas basada en direcciones de correo electrónico no se puede utilizar con ninguna otra identidad de certificado.

Para habilitar la detección de cuentas basada en direcciones de correo electrónico cuando se trata de usuarios que se conectan desde fuera de la red corporativa, también debe configurar NetScaler Gateway con los datos de conexión de StoreFront. Para obtener más información, consulte Conexión a StoreFront mediante la detección basada en direcciones de correo electrónico.

Cómo agregar un registro SRV a un servidor DNS

1. En la pantalla **Inicio**, haga clic en **Herramientas administrativas** y, en la carpeta **Herramientas administrativas**, haga clic en **DNS**.
2. En el panel izquierdo del **Administrador de DNS**, seleccione un dominio en las zonas de búsqueda directa o inversa. Haga

clic con el botón secundario y seleccione **Otros registros nuevos**.
3. En el cuadro de diálogo **Tipo de registro del recurso**, seleccione **Ubicación del servicio (SRV)** y, a continuación, haga clic en **Crear registro**.
4. En el cuadro de diálogo **Nuevo registro de recursos**, introduzca el valor de host **_citrixreceiver** en el cuadro **Servicio**.
5. En el cuadro **Protocolo** , introduzca el valor **_tcp**.
6. En el cuadro **Host que ofrece este servicio**, especifique el FQDN y el puerto para el dispositivo NetScaler Gateway (para dar respaldo a usuarios locales y remotos) o el servidor StoreFront (para dar respaldo solo a los usuarios de la red local) con el formato *nombre de servidor.dominio:puerto*.
   Si el entorno contiene servidores DNS internos y externos, es posible agregar un registro SRV donde se especifique el FQDN del servidor StoreFront en el servidor DNS interno y otro registro donde se especifique el FQDN de NetScaler Gateway en el servidor externo. Con esta configuración, los usuarios de la red local reciben la información de StoreFront, mientras que los usuarios remotos reciben los datos de conexión de NetScaler Gateway.
7. Si ha configurado un registro SRV para el dispositivo NetScaler Gateway, agregue los datos de conexión de StoreFront a NetScaler Gateway en una configuración global o un perfil de sesión.

Sitios de Citrix Receiver para Web

Los usuarios con exploradores Web compatibles pueden acceder a las tiendas de StoreFront navegando a sitios de Citrix Receiver para Web. Al crear una nueva tienda, se crea automáticamente un sitio de Citrix Receiver para Web vinculado a la tienda. La configuración predeterminada de los sitios de Citrix Receiver para Web requiere que se instale una versión compatible de Citrix Receiver para acceder a sus escritorios y aplicaciones. Para obtener más información acerca de las combinaciones de Citrix Receiver y explorador Web que pueden usarse con el fin de acceder a sitios de Citrix Receiver para Web, consulte Requisitos del dispositivo del usuario.

De forma predeterminada, cuando un usuario accede a un sitio de Citrix Receiver para Web desde un equipo con Windows o Mac OS X, el sitio intenta determinar si Citrix Receiver está instalado en el dispositivo de usuario. Si no se detecta Citrix Receiver, se solicita al usuario que descargue e instale la versión de Citrix Receiver correspondiente a su plataforma. La ubicación de descarga predeterminada es el sitio Web de Citrix, pero también puede, en su lugar, copiar los archivos de instalación al servidor StoreFront y proporcionar a los usuarios estos archivos locales. El almacenamiento local de los archivos de instalación de Citrix Receiver le permite configurar el sitio para ofrecer a los usuarios con clientes de versiones anteriores la posibilidad de actualizar su versión a la versión del servidor. Para obtener más información acerca de la configuración de la implementación de Citrix Receiver para Windows y Citrix Receiver para Mac, consulte Configuración de sitios de Citrix Receiver para Web.

Citrix Receiver para HTML5

Citrix Receiver para HTML5 es un componente de StoreFront que está integrado de manera predeterminada en los sitios de Citrix Receiver para Web. Puede habilitar Citrix Receiver para HTML5 en los sitios de Citrix Receiver para Web, de modo que los usuarios puedan acceder a los recursos aunque no puedan instalar Citrix Receiver. Citrix Receiver para HTML5 permite que los usuarios puedan acceder a escritorios y aplicaciones directamente con exploradores Web compatibles con HTML5 sin necesidad de instalar Citrix Receiver. Cuando se crea un sitio, Citrix Receiver para HTML5 está inhabilitado de forma predeterminada. Para obtener más información sobre la habilitación de Citrix Receiver para HTML5, consulte citrix-receiver-download-page-template.html.

Para acceder a sus escritorios y aplicaciones usando Citrix Receiver para HTML5, los usuarios deben acceder al sitio de Citrix Receiver para Web con un explorador Web compatible con HTML5. Para obtener más información acerca de los sistemas operativos y exploradores Web que pueden usarse con Citrix Receiver para HTML5, consulte Requisitos del dispositivo del usuario.

Citrix Receiver para HTML5 está disponible tanto para usuarios de la red interna como para usuarios remotos que se conectan a través de NetScaler Gateway. En caso de conexiones desde la red interna, Citrix Receiver para HTML5 solo admite el acceso a escritorios y aplicaciones proporcionados por un subconjunto de productos respaldados por los sitios de Citrix Receiver para Web. Los usuarios que se conectan a través de NetScaler Gateway pueden acceder a recursos suministrados por una gama más amplia de productos si se eligió Citrix Receiver para HTML5 como una opción al configurar StoreFront. Se requieren versiones específicas de NetScaler Gateway para usarlo con Citrix Receiver para HTML5. Para obtener más información, consulte Requisitos de infraestructura.

De manera predeterminada, el acceso a través de Citrix Receiver para HTML5 para los recursos proporcionados por XenDesktop y XenApp se encuentra inhabilitado para los usuarios locales de la red interna. Para habilitar el acceso local a escritorios y aplicaciones mediante Citrix Receiver para HTML5, debe habilitar la directiva Conexiones de WebSockets en los servidores XenDesktop y XenApp. Asegúrese de que los firewalls y otros dispositivos de red permiten el acceso al puerto de Citrix Receiver para HTML5 especificado en la directiva. Para obtener más información, consulte Configuraciones de directiva de WebSockets.

De forma predeterminada, Citrix Receiver para HTML5 inicia los escritorios y las aplicaciones en una nueva pestaña del explorador. No obstante, cuando los usuarios inician recursos con Citrix Receiver para HTML5 a partir de accesos directos, el escritorio o la aplicación reemplazan el sitio de Citrix Receiver para Web en la pestaña existente del explorador en vez de aparecer en una nueva pestaña. Puede configurar Citrix Receiver para HTML5 para que los recursos se inicien siempre en la misma pestaña del sitio de Receiver para Web. Para obtener más información, consulte Configuración del uso de las pestañas del explorador Web con Citrix Receiver para HTML5.

Accesos directos a los recursos

Puede generar direcciones URL de acceso a escritorios y aplicaciones, de modo que se pueda acceder a ellos a través de sitios de Citrix Receiver para Web. Inserte estos enlaces en los sitios Web alojados en la red interna y los usuarios tendrán acceso inmediato a los recursos. Los usuarios hacen clic en un enlace y se les redirige al sitio de Receiver para Web, donde deben iniciar sesión si todavía no lo han hecho. El sitio de Citrix Receiver para Web inicia automáticamente el recurso. En el caso de las aplicaciones, los usuarios también se suscriben a ellas si no lo han hecho anteriormente. Para obtener más información acerca de la generación de accesos directos a recursos, consulte Configuración de sitios de Citrix Receiver para Web.

Como con todos los escritorios y aplicaciones a los que se accede a través de sitios de Citrix Receiver para Web, los usuarios deben tener instalado Citrix Receiver o deben usar Citrix Receiver para HTML5 si desean acceder a los recursos a través de accesos directos. El método utilizado por un sitio de Citrix Receiver para Web depende de cómo esté configurado el sitio, de si se detecta la presencia de Citrix Receiver en los dispositivos de los usuarios y de si se está usando un explorador compatible con HTML5. Por motivos de seguridad, es posible que los usuarios de Internet Explorer tengan que confirmar que desean iniciar los recursos a los que se accede a través de accesos directos. Indique a los usuarios que agreguen el sitio de Receiver para Web a la zona de Intranet local o Sitios de confianza en Internet Explorer para evitar este paso adicional. De forma predeterminada, tanto el control del espacio de trabajo como el inicio automático del escritorio están inhabilitados cuando los usuarios acceden a los sitios de Citrix Receiver para Web a través de accesos directos.

Al crear el acceso directo a una aplicación, asegúrese de que no haya otras aplicaciones del sitio de Citrix Receiver para Web que tengan el mismo nombre. Los accesos directos no pueden distinguir varias instancias de una aplicación con el mismo nombre. Del mismo modo, si desea que varias instancias de un escritorio estén disponibles desde un solo grupo de escritorios desde el sitio de Citrix Receiver para Web, no puede crear accesos directos independientes para cada instancia. Los accesos directos no pueden pasar parámetros de línea de comandos a las aplicaciones.

Para crear accesos directos de aplicaciones, se puede configurar StoreFront con las direcciones URL de los sitios Web internos que alojarán los accesos directos. Cuando un usuario hace clic en el acceso directo de una aplicación en un sitio Web, StoreFront coteja ese sitio Web con la lista de direcciones URL que ha indicado para asegurarse de que la solicitud proviene de un sitio Web de confianza. Sin embargo, los sitios Web que alojan accesos directos no se validan cuando se trata de usuarios que se conectan a través de NetScaler Gateway porque las direcciones URL no se transfieren a StoreFront. Para asegurarse de que los usuarios remotos puedan acceder a accesos directos de aplicaciones de sitios Web internos y de confianza, configure NetScaler Gateway para limitar el acceso de los usuarios a solamente esos sitios específicos. Para obtener más información, consulte http://support.citrix.com/article/CTX123610.

Personalización de los sitios

Los sitios de Citrix Receiver para Web ofrecen un mecanismo para personalizar la interfaz de usuario. Puede personalizar las cadenas de texto, la hoja de estilo en cascada y los archivos de JavaScript. También puede agregar pantallas personalizadas que se mostrarán antes y después del inicio de sesión, así como paquetes de idioma.

Consideraciones importantes

Los usuarios que accedan a las tiendas a través de un sitio de Citrix Receiver para Web se benefician de muchas de las funciones disponibles mediante el acceso a tiendas con Citrix Receiver, tales como la sincronización de aplicaciones. A la hora de optar por utilizar los sitios de Citrix Receiver para Web para proporcionar a los usuarios acceso a las tiendas, tenga en cuenta las siguientes restricciones.

- A través de un sitio de Citrix Receiver para Web solo se puede acceder a una única tienda.
- Los sitios de Citrix Receiver para Web no pueden iniciar conexiones de red privada virtual (VPN) con SSL (Secure Sockets Layer). Los usuarios que inician sesión a través de NetScaler Gateway sin una conexión VPN no pueden acceder a las aplicaciones Web para las que App Controller exige utilizar conexiones VPN.
- Las aplicaciones suscritas no están disponibles en el menú Inicio de Windows cuando se accede a una tienda mediante un sitio de Citrix Receiver para Web.
- La asociación de tipos de archivo no está disponible entre los documentos locales y las aplicaciones alojadas en servidores, a las que se accede mediante un sitio de Citrix Receiver para Web.
- No se puede acceder a aplicaciones sin conexión a través de sitios de Citrix Receiver para Web.
- Los sitios de Citrix Receiver para Web no admiten productos de Citrix Online integrados en las tiendas. Los productos de Citrix Online deben entregarse con App Controller u ofrecerse como aplicaciones alojadas para permitir el acceso a ellos mediante los sitios de Citrix Receiver para Web.
- Citrix Receiver para HTML5 se puede usar sobre conexiones HTTPS si el VDA es XenApp 7.6 o XenDesktop 7.6 y tiene SSL habilitado, o si el usuario se conecta usando NetScaler Gateway.
- Para utilizar Citrix Receiver para HTML5 con Mozilla Firefox con conexión HTTPS, los usuarios deben escribir about:config en la barra de direcciones de Firefox y establecer la preferencia network.websocket.allowInsecureFromHTTPS en true.

Sitios de Desktop Appliance

Los usuarios con dispositivos de escritorio que no están unidos a ningún dominio pueden acceder a los escritorios a través de los sitios de Desktop Appliance. En este contexto, la no pertenencia a un dominio se refiere a dispositivos que no se han vinculado a ningún dominio del bosque de Active Directory que contiene los servidores StoreFront.

Cuando se crea una tienda para una implementación de XenDesktop mediante Citrix Studio, también se crea de forma predeterminada un sitio de Desktop Appliance para la tienda. Los sitios de Desktop Appliance se crean de forma predeterminada solamente cuando StoreFront se instala y configura como parte de una instalación de XenDesktop. Puede

crear los sitios de Desktop Appliance manualmente mediante comandos de Windows PowerShell. Para obtener más información, consulte Configuración de los sitios de Desktop Appliance.

Los sitios de Desktop Appliance ofrecen una experiencia de usuario similar al inicio de sesión en un escritorio local. Los exploradores Web de los dispositivos de escritorio se configuran para iniciarse en modo de pantalla completa y mostrar la pantalla de inicio de sesión para el sitio de Desktop Appliance. Cuando un usuario inicia sesión en un sitio, de forma predeterminada, se inicia automáticamente el primer escritorio (por orden alfabético) disponible para el usuario de la tienda para la que se ha configurado el sitio. Si proporciona a los usuarios acceso a varios escritorios de una tienda, puede configurar el sitio de Desktop Appliance para que muestre todos los escritorios disponibles. De esta manera, los usuarios pueden elegir el escritorio al que acceder. Para obtener más información, consulte Configuración de los sitios de Desktop Appliance.

Cuando se inicia el escritorio de un usuario, aparece en modo de pantalla completa y oculta el explorador Web. La sesión del usuario se cierra automáticamente desde el sitio de Desktop Appliance. Cuando el usuario cierra sesión en el escritorio, aparece de nuevo el explorador Web, con la pantalla de inicio de sesión del sitio de Desktop Appliance. Cuando un escritorio se inicia, aparece un mensaje que contiene un vínculo para reiniciar el escritorio si no se puede acceder a él. Si desea habilitar esta funcionalidad, configure el grupo de entrega para permitir a los usuarios reiniciar sus escritorios. Para obtener más información, consulte Grupos de entrega.

Para proporcionar acceso a los escritorios, se necesita una versión compatible de Citrix Receiver en el dispositivo de escritorio. Por lo general, los proveedores de dispositivos compatibles con XenDesktop integran Citrix Receiver en sus productos. En caso de dispositivos Windows, también debe instalar Citrix Desktop Lock y configurarlo con la dirección URL para el sitio de Desktop Appliance. Si se utiliza Internet Explorer, se debe agregar el sitio de Desktop Appliance a las zonas de Intranet local o sitios de confianza. Para obtener más información sobre Citrix Desktop Lock, consulte Cómo impedir el acceso del usuario al escritorio local.

Consideraciones importantes

Los sitios de Desktop Appliance están pensados para los usuarios locales de la red interna que acceden a los escritorios desde dispositivos de escritorio no unidos a ningún dominio. A la hora de optar por utilizar los sitios de Desktop Appliance para proporcionar a los usuarios acceso a las tiendas, tenga en cuenta las siguientes restricciones.

- Si piensa implementar dispositivos de escritorio unidos a dominios y equipos reasignados, no los configure para acceder a las tiendas a través de los sitios de Desktop Appliance. Aunque puede configurar Citrix Receiver con la URL de servicios XenApp para la tienda, se recomienda usar el nuevo Desktop Lock tanto para los casos de uso de dispositivos que pertenecen a un dominio como para los que no pertenecen a un dominio. Para obtener más información, consulte Citrix Receiver Desktop Lock.
- Los sitios de Desktop Appliance no respaldan las conexiones de usuarios remotos de fuera de la red corporativa. Los usuarios que inician sesión en NetScaler Gateway no pueden acceder a los sitios de Desktop Appliance.

Direcciones URL de servicios XenApp

Los usuarios con versiones anteriores de clientes Citrix que no se pueden actualizar pueden acceder a las tiendas mediante la configuración de sus clientes con la URL de servicios XenApp para una tienda. También puede habilitar el acceso a las tiendas a través de las direcciones URL de servicios XenApp desde dispositivos de escritorio unidos a un dominio y equipos reasignados que ejecutan Citrix Desktop Lock. En este contexto, la unión a un dominio se refiere a dispositivos que se han vinculado a un dominio del bosque de Active Directory que contiene los servidores StoreFront.

StoreFront admite la autenticación PassThrough con tarjetas de proximidad a través de Citrix Receiver para las direcciones

URL de servicios XenApp. Los productos asociados de Citrix Ready utilizan Citrix Fast Connect API para optimizar los inicios de sesión de los usuarios para la conexión a través de Citrix Receiver para Windows a las tiendas mediante la URL de servicios XenApp. Los usuarios se autentican en estaciones de trabajo mediante tarjetas de proximidad y se conectan rápidamente a los escritorios y las aplicaciones que proporcionan XenDesktop y XenApp. Para obtener más información, consulte la documentación más reciente de Citrix Receiver para Windows.

Al crear una nueva tienda, la URL de servicios XenApp correspondiente está habilitada de forma predeterminada. La URL de servicios XenApp de una tienda tiene el formato http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, donde serveraddress es el nombre de dominio completo del servidor o entorno de equilibrio de carga de la implementación de StoreFront y storename es el nombre especificado para la tienda cuando se creó. Esto permite que los Citrix Receivers que solo pueden usar el protocolo PNAgent puedan conectarse a StoreFront. Para conocer qué clientes pueden utilizarse para acceder a tiendas mediante direcciones URL de servicios XenApp, consulte Requisitos del dispositivo del usuario.

Consideraciones importantes

Las direcciones URL de servicios XenApp se han diseñado para los usuarios que no pueden actualizarse a Citrix Receiver y para los casos en que no están disponibles otros métodos de acceso. A la hora de optar por utilizar las direcciones URL de servicios XenApp para proporcionar a los usuarios acceso a las tiendas, tenga en cuenta las siguientes restricciones.

- No se puede modificar la URL de servicios XenApp para una tienda.
- No se puede modificar la configuración de la URL de servicios XenApp mediante la edición del archivo de configuración, config.xml.
- Las direcciones URL de servicios XenApp respaldan la autenticación explícita, la autenticación PassThrough de dominio, la autenticación con tarjeta inteligente y la autenticación PassThrough con tarjeta inteligente. La autenticación explícita está habilitada de forma predeterminada. Solo se puede configurar un método de autenticación para cada dirección URL de servicios XenApp, y solo está disponible una dirección URL por tienda. Para habilitar varios métodos de autenticación, debe crear tiendas independientes, cada una con una URL de servicios XenApp, para cada método de autenticación. Los usuarios deben conectarse a la tienda adecuada para su método de autenticación. Para obtener más información, consulte Autenticación basada en XML.
- El control del espacio de trabajo está habilitado de forma predeterminada para las direcciones URL de servicios XenApp y no se puede configurar ni inhabilitar.
- Las solicitudes de los usuarios para cambiar sus contraseñas se enrutan al controlador de dominio de forma directa a través de servidores de XenDesktop, XenApp y XenApp que proporcionan escritorios y aplicaciones para la tienda. De esta forma, se omite el servicio de autenticación de StoreFront.

Autenticación de usuario

Aug 14, 2017

StoreFront respalda diversos métodos de autenticación para los usuarios que acceden a las tiendas, aunque no todos estén disponibles, ya que dependen del método de acceso de los usuarios y de su ubicación de red. Por motivos de seguridad, algunos de los métodos de autenticación están inhabilitados de forma predeterminada cuando se crea la primera tienda. Para obtener más información sobre cómo habilitar e inhabilitar los métodos de autenticación de usuarios, consulte Creación y configuración del servicio de autenticación.

Nombre de usuario y contraseña

Los usuarios deben introducir sus credenciales y autenticarse cuando acceden a las tiendas. La autenticación explícita está habilitada de forma predeterminada. Todos los métodos de acceso de usuario son compatibles con la autenticación explícita.

Cuando un usuario emplea NetScaler Gateway para acceder a Citrix Receiver para Web, NetScaler Gateway se ocupa del inicio de sesión y del cambio de contraseña cuando ésta caduca. Los usuarios pueden cambiar sus contraseñas siempre que quieran mediante la interfaz de usuario de Citrix Receiver para Web. Después de un cambio de contraseña a petición del usuario, la sesión de NetScaler Gateway termina y el usuario tiene que volver a iniciar la sesión. Los usuarios de Citrix Receiver para Linux pueden cambiar únicamente las contraseñas caducadas.

Autenticación SAML

Los usuarios se autentican en un proveedor de identidades SAML y su sesión se inicia automáticamente cuando acceden a sus tiendas. StoreFront puede admitir la autenticación SAML directamente dentro de la red corporativa, sin tener que ir a través de NetScaler.

SAML (Security Assertion Markup Language) es un estándar abierto utilizado por los productos de identidad y autenticación, como Microsoft AD FS (servicios de federación de Active Directory). Con la integración de la autenticación SAML a través de StoreFront, los administradores pueden permitir que los usuarios, por ejemplo, inicien sesión una vez en la red de la empresa y, a continuación, aplicar el inicio de sesión único Single Sign-on en las aplicaciones publicadas.

Requisitos:

- Implementación del servicio de autenticación federada de Citrix.
- Proveedores de identidades (IdPs) compatibles con SAML 2.0:
  - Microsoft AD FS v4.0 (Windows Server 2016) usando solo enlaces SAML (enlaces que no sean de WS-Federation). Para más información, consulte Microsoft AD FS 2016 Deployment and Microsoft AD 2016 FS Operations.
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - Microsoft AD FS v2.0 (Windows Server 2008 R2)
  - NetScaler Gateway (configurado como proveedor de identidades - IdP)
- Configure la autenticación SAML en StoreFront usando la consola de administración de StoreFront en una nueva implementación (consulte Creación de una nueva implementación), o en una implementación existente (consulte Configuración del servicio de autenticación). También puede configurar la autenticación de SAML mediante cmdlets de PowerShell, consulte SDK de StoreFront .
- Citrix Receiver para Windows (4.6 o posterior) y Citrix Receiver para Web.

El uso de SAML la autenticación con NetScaler recibe respaldo actualmente con sitios de Receiver para Web.

PassThrough de dominio

Los usuarios realizan la autenticación en equipos Windows que no pertenecen a un dominio, y sus credenciales se usan para iniciar sesión automáticamente cuando acceden a las tiendas. Al instalar StoreFront, la autenticación PassThrough de dominio se inhabilita de forma predeterminada. La autenticación PassThrough de dominio puede estar habilitada para los usuarios que se conectan a las tiendas a través de Citrix Receiver y de direcciones URL de servicios XenApp. Los sitios de Citrix Receiver para Web respaldan la autenticación PassThrough de dominio únicamente para Internet Explorer. Habilite la autenticación PassThrough de dominio en el nodo del sitio de Receiver para Web que hay en la consola de administración. Necesitará configurar SSON en Citrix Receiver para Windows. Citrix Receiver para HTML5 no respalda la autenticación PassThrough de dominio. Para usar la autenticación PassThrough de dominio, los usuarios necesitan Citrix Receiver para Windows o el Online Plug-in para Windows. La autenticación PassThrough debe estar habilitada cuando se instalan Citrix Receiver para Windows o el Online Plug-in para Windows en los dispositivos de los usuarios.

Método de autenticación PassThrough desde NetScaler Gateway

Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas. La autenticación PassThrough desde NetScaler Gateway está habilitada de forma predeterminada al configurar el acceso remoto a una tienda. Los usuarios pueden conectarse a través de NetScaler Gateway a las tiendas usando Citrix Receiver o usando sitios de Citrix Receiver para Web. Los sitios de Desktop Appliance no admiten las conexiones a través de NetScaler Gateway. Para obtener más información acerca de la configuración de StoreFront para NetScaler Gateway, consulte Cómo agregar una conexión de NetScaler Gateway.

StoreFront admite la autenticación PassThrough con los siguientes métodos de autenticación de NetScaler Gateway.

- **Token de seguridad.** Los usuarios inician sesión en NetScaler Gateway mediante códigos de acceso derivados de códigos generados por tokens de seguridad, y combinados, en algunos casos, con números de identificación personales (PIN). Si habilita la autenticación PassThrough con token de seguridad solamente, asegúrese de que los recursos disponibles no requieren formas de autenticación adicionales o alternativas, como credenciales de dominio de Microsoft Active Directory.
- **Dominio y token de seguridad.** Los usuarios que inician sesión en NetScaler Gateway deben introducir sus credenciales de dominio y los códigos de acceso de tokens de seguridad.
- **Certificado del cliente.** Los usuarios inician sesión en NetScaler Gateway y su autenticación se produce basándose en los atributos del certificado del cliente que se presenta ante NetScaler Gateway. Configure la autenticación de certificados del cliente para permitir que los usuarios inicien sesión en NetScaler Gateway usando tarjetas inteligentes. La autenticación de certificados del cliente también puede utilizarse con otros tipos de autenticación para ofrecer autenticación de doble origen.

StoreFront usa el servicio de autenticación de NetScaler Gateway para proporcionar autenticación PassThrough a los usuarios remotos, para que estos usuarios solo deban introducir sus credenciales una vez. Sin embargo, de forma predeterminada, la autenticación PassThrough solo está habilitada para los usuarios que inician sesión en NetScaler Gateway con una contraseña. Para configurar la autenticación PassThrough desde NetScaler Gateway para el acceso a StoreFront por parte de usuarios de tarjeta inteligente, delegue la validación de credenciales en NetScaler Gateway. Para obtener más información, consulte Creación y configuración del servicio de autenticación.

Los usuarios pueden conectarse a tiendas en Citrix Receiver con la autenticación PassThrough a través del túnel VPN SSL mediante NetScaler Gateway Plug-in. Los usuarios remotos que no pueden instalar NetScaler Gateway Plug-in pueden utilizar el acceso sin cliente para conectarse a las tiendas en Citrix Receiver con la autenticación PassThrough. Para utilizar el acceso sin cliente con el fin de conectarse a las tiendas, los usuarios necesitan una versión de Citrix Receiver que admita el acceso sin cliente.

Además, es posible habilitar el acceso sin cliente con la autenticación PassThrough en sitios de Citrix Receiver para Web. Para hacer esto, configure NetScaler Gateway de modo que funcione como proxy remoto seguro. Los usuarios inician sesión directamente en NetScaler Gateway y usan el sitio de Citrix Receiver para Web para acceder a sus aplicaciones sin necesidad de volver a autenticarse.

Los usuarios que se conectan a recursos de App Controller con el acceso sin cliente solo pueden acceder a las aplicaciones de software como servicio (SaaS) externas. Para acceder a las aplicaciones Web internas, los usuarios remotos deben utilizar NetScaler Gateway Plug-in.

Si desea configurar la autenticación de doble origen en NetScaler Gateway para usuarios remotos que accedan a las tiendas desde Citrix Receiver, debe crear dos directivas de autenticación en NetScaler Gateway. Configure RADIUS (Servicio de autenticación remota telefónica de usuario) como el método principal de autenticación y LDAP (Protocolo ligero de acceso a directorios) como el método secundario. Modifique el índice de credenciales para usar el método secundario de autenticación en el perfil de sesión, de manera que las credenciales de LDAP se transfieran a StoreFront. Al agregar un dispositivo NetScaler Gateway a la configuración de StoreFront, establezca el Tipo de inicio de sesión en Dominio y token de seguridad. Para obtener más información, consulte http://support.citrix.com/article/CTX125364.

Para habilitar la autenticación en varios dominios de StoreFront mediante NetScaler Gateway, establezca SSO Name Attribute como userPrincipalName en la directiva de autenticación de LDAP de NetScaler Gateway para cada dominio. Es posible que deba especificar un dominio a los usuarios en la página de inicio de sesión de NetScaler Gateway para que se pueda determinar la directiva de LDAP correspondiente. Al configurar los perfiles de sesión de NetScaler Gateway para las conexiones con StoreFront, no especifique un dominio Single Sign-On. Debe configurar las relaciones de confianza entre cada uno de los dominios. Asegúrese de permitir que los usuarios inicien sesión en StoreFront desde cualquier dominio al no restringir el acceso a solo aquellos dominios que sean explícitamente de confianza.

Cuando la implementación de NetScaler Gateway lo respalde, puede utilizar SmartAccess para controlar el acceso de los usuarios a los recursos de XenDesktop y XenApp en función de las directivas de sesión de NetScaler Gateway. Para obtener más información acerca de SmartAccess, consulte How SmartAccess works for XenApp and XenDesktop.

Tarjetas inteligentes

Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a las tiendas. Al instalar StoreFront, la autenticación con tarjeta inteligente se inhabilita de forma predeterminada. La autenticación con tarjeta inteligente puede habilitarse para los usuarios que se conectan a las tiendas a través de Citrix Receiver, Citrix Receiver para Web, los sitios de Desktop Appliance y las direcciones URL de servicios XenApp.

La autenticación con tarjeta inteligente optimiza el proceso de inicio de sesión de los usuarios y mejora la seguridad del acceso de los usuarios a la infraestructura. El acceso a la red corporativa interna está protegido por la autenticación de dos fases basada en un certificado con infraestructura de clave pública. Las claves privadas están protegidas por controles de hardware y nunca salen de la tarjeta inteligente. Los usuarios obtienen la comodidad de acceder a sus escritorios y aplicaciones desde una serie de dispositivos de la empresa con sus tarjetas inteligentes y sus PIN.

Puede usar tarjetas inteligentes para la autenticación de usuarios a través de StoreFront en los escritorios y las aplicaciones que proporcionan XenDesktop y XenApp. Los usuarios de tarjetas inteligentes que inician sesión en StoreFront también pueden acceder a las aplicaciones proporcionadas por App Controller. No obstante, los usuarios deben volver a autenticarse para acceder a las aplicaciones Web de App Controller que usan la autenticación de certificados del cliente.

Para habilitar la autenticación con tarjeta inteligente, las cuentas de los usuarios deben configurarse ya sea en el dominio de Microsoft Active Directory que contiene los servidores StoreFront, o bien, en un dominio que tenga una relación de confianza bidireccional directa con el dominio del servidor StoreFront. Se respaldan las implementaciones multibosque de

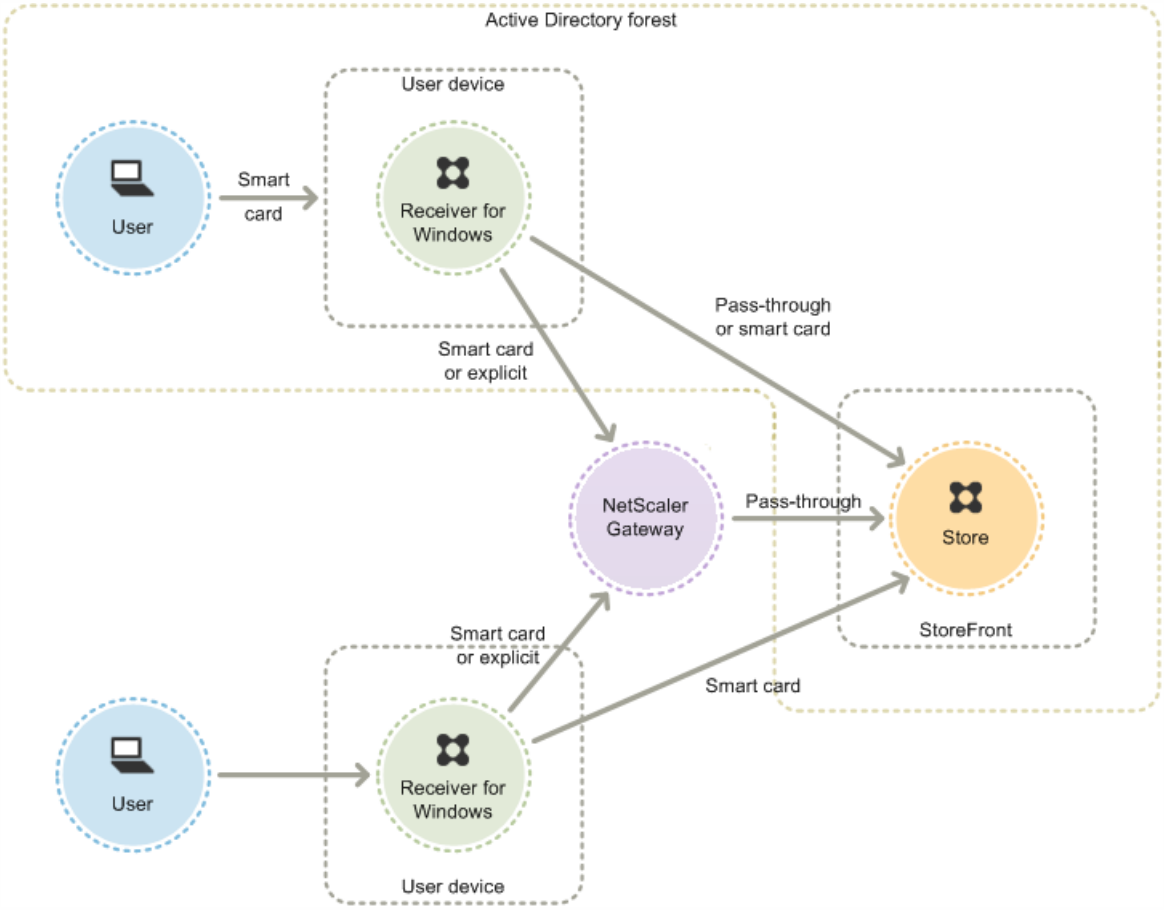
confianza bidireccional.

La configuración de la autenticación con tarjeta inteligente para StoreFront depende de los dispositivos del usuario, de los clientes instalados y de si los dispositivos están unidos a un dominio o no. En este contexto, la unión a un dominio se refiere a dispositivos que se han vinculado a un dominio del bosque de Active Directory que contiene los servidores StoreFront.

Uso de tarjetas inteligentes con Citrix Receiver para Windows

Los usuarios con dispositivos que ejecutan Citrix Receiver para Windows se pueden autenticar con tarjetas inteligentes, ya sea directamente o a través de NetScaler Gateway. Se pueden usar tanto los dispositivos que están unidos a un dominio como los que no, aunque la experiencia de usuario es un poco diferente en cada caso.

La ilustración muestra las opciones para la autenticación con tarjeta inteligente a través de Citrix Receiver para Windows.



Para los usuarios locales con dispositivos unidos a dominio, puede configurar la autenticación con tarjeta inteligente de forma que solo se pidan las credenciales de usuario una vez. Los usuarios inician la sesión en sus dispositivos usando sus tarjetas inteligentes y sus PIN y, con la configuración adecuada, no se les vuelve a pedir el PIN. Los usuarios se autentican de forma silenciosa en StoreFront y también en sus escritorios y aplicaciones. Para conseguir esto, configure Citrix Receiver para Windows con autenticación PassThrough y habilite la autenticación PassThrough de dominio en StoreFront.

Los usuarios inician sesión en sus dispositivos y, a continuación, se autentican en Citrix Receiver para Windows con sus PIN. No hay más solicitudes de PIN cuando intentan iniciar aplicaciones y escritorios

Como los usuarios de dispositivos que no pertenecen a un dominio inician sesión en Citrix Receiver para Windows directamente, puede permitir que los usuarios recurran a la autenticación explícita. Si se configura tanto la autenticación

explícita como la autenticación con tarjeta inteligente, primero se solicita a los usuarios que inicien sesión con sus tarjetas inteligentes y sus PIN. En caso de problemas con las tarjetas inteligentes, también tendrán la opción de seleccionar la autenticación explícita.

Los usuarios que se conectan a través de NetScaler Gateway deben iniciar la sesión usando su tarjeta inteligente y su PIN al menos dos veces para acceder a sus escritorios y aplicaciones. Esto se aplica a dispositivos unidos a un dominio y a dispositivos que no pertenecen a ningún dominio. Los usuarios se autentican usando su tarjeta inteligente y su PIN y, con la configuración apropiada, solo tienen que volver a introducir su PIN cuando acceden a sus escritorios y aplicaciones. Para conseguir esto, hay que habilitar la autenticación PassThrough con NetScaler Gateway en StoreFront y delegar la validación de credenciales en NetScaler Gateway. Después, cree un servidor virtual adicional de NetScaler Gateway a través del cual se enrutarán las conexiones de usuario hacia sus recursos. En el caso de dispositivos unidos a un dominio, también debe configurar Citrix Receiver para Windows para la autenticación PassThrough.

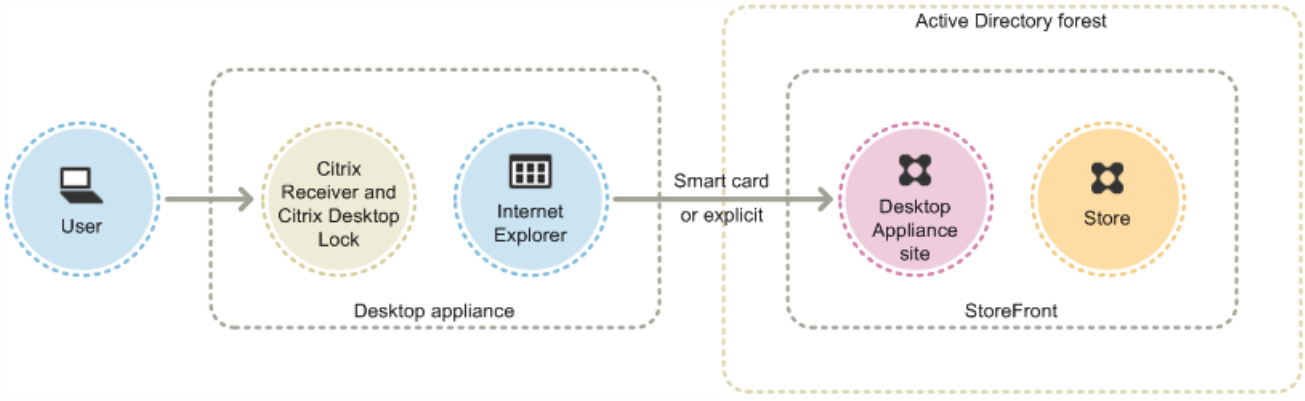
Nota: Si utiliza Citrix Receiver para Windows 4.2, la versión actual, puede configurar un segundo servidor virtual y usar la puerta de enlace óptima para eliminar la necesidad de solicitar el PIN al iniciar aplicaciones y escritorios.

Los usuarios pueden iniciar sesión en NetScaler Gateway con su tarjeta inteligente y su PIN o con credenciales explícitas. Esto permite ofrecer a los usuarios la opción de recurrir a la autenticación explícita para iniciar sesión con NetScaler Gateway. Configure la autenticación PassThrough de NetScaler Gateway a StoreFront y delegue la validación de las credenciales a NetScaler Gateway para los usuarios de tarjeta inteligente de modo que los usuarios se autentiquen silenciosamente en StoreFront.

Uso de tarjetas inteligentes con los sitios de Desktop Appliance

Los dispositivos de escritorio Windows que no están unidos a ningún dominio se pueden configurar para permitir que los usuarios inicien sesión en los escritorios usando las tarjetas inteligentes. El dispositivo debe tener Citrix Desktop Lock y se debe utilizar Internet Explorer para acceder al sitio de Desktop Appliance.

La ilustración muestra la autenticación con tarjeta inteligente desde un dispositivo de escritorio que no está unido a ningún dominio.



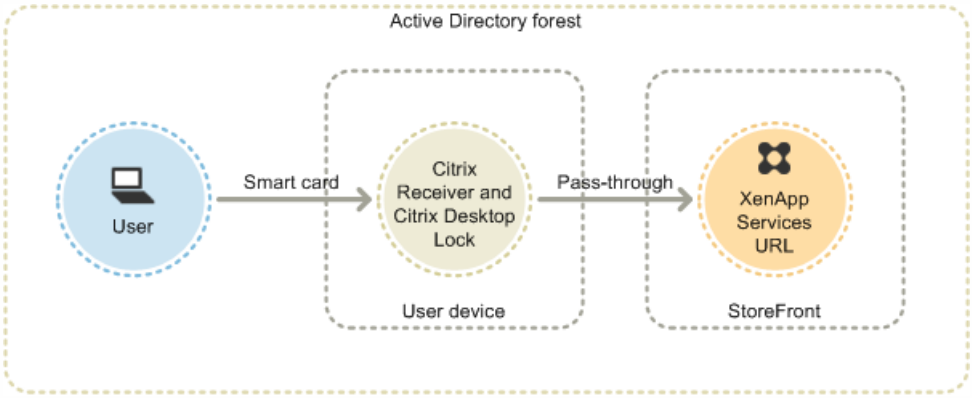
Cuando los usuarios acceden a dispositivos Desktop Appliance, Internet Explorer se inicia en modo de pantalla completa y el usuario puede ver la pantalla de inicio de sesión del sitio de Desktop Appliance. Los usuarios se autentican en el sitio mediante sus tarjetas inteligentes y sus PIN. Si el sitio de Desktop Appliance está configurado para la autenticación PassThrough, los usuarios se autentican automáticamente cuando acceden a sus escritorios y aplicaciones. No se vuelven a solicitar los PIN a los usuarios. Sin la autenticación PassThrough, los usuarios deben introducir sus PIN por segunda vez cuando inicien un escritorio o aplicación.

Puede permitir que los usuarios utilicen la autenticación explícita si tienen problemas con las tarjetas inteligentes. Para ello, configure el sitio de Desktop Appliance para ambos: las tarjetas inteligentes y la autenticación explícita. En esta configuración, la autenticación con tarjeta inteligente es el método de acceso principal, por lo que los usuarios primero deben introducir sus PIN. No obstante, el sitio también proporciona un vínculo que permite a los usuarios iniciar sesión con credenciales explícitas.

Uso de tarjetas inteligentes con las direcciones URL de servicios XenApp

Los usuarios de dispositivos de escritorio unidos a un dominio y de equipos reasignados que ejecutan Citrix Desktop Lock se pueden autenticar mediante tarjetas inteligentes. A diferencia de otros métodos de acceso, la autenticación PassThrough de credenciales con tarjeta inteligente se habilita automáticamente cuando se configura la autenticación con tarjeta inteligente para una URL de servicios XenApp.

La ilustración muestra la autenticación con tarjeta inteligente desde un dispositivo unido a un dominio que ejecuta Citrix Desktop Lock.



Los usuarios inician sesión en los dispositivos con las tarjetas inteligentes y los PIN. A continuación, Citrix Desktop Lock autentica de manera silenciosa a los usuarios en StoreFront a través de la URL de servicios XenApp. Los usuarios se autentican automáticamente cuando acceden a los escritorios y aplicaciones, y no se les vuelve a pedir el PIN.

Uso de tarjetas inteligentes con Citrix Receiver para Web

Puede habilitar la autenticación con tarjeta inteligente en Citrix Receiver para Web desde la consola de administración de StoreFront.

1. Seleccione el nodo Citrix Receiver para Web del panel de la izquierda.
2. Seleccione el sitio en el que quiere usar la autenticación con tarjeta inteligente.
3. Seleccione la tarea Elegir métodos de autenticación del panel de la derecha.
4. Marque la casilla Tarjeta inteligente en la pantalla de diálogo emergente y haga clic en Aceptar.

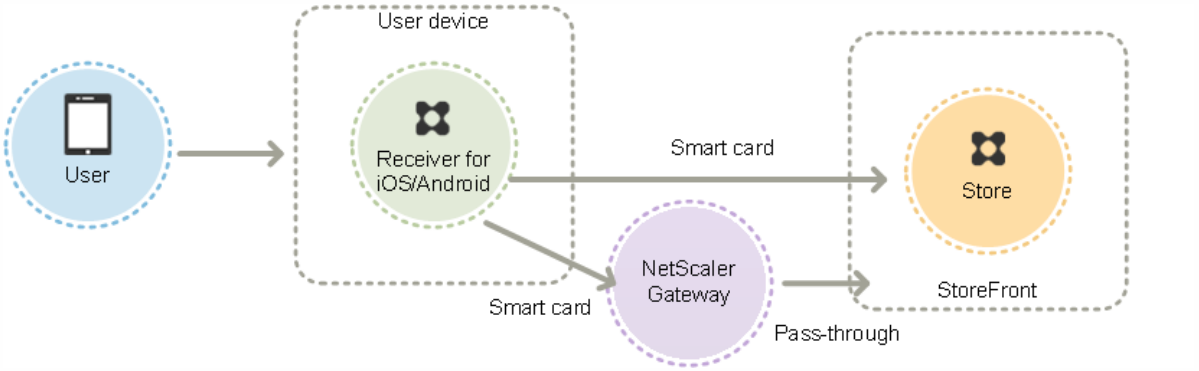
Si habilita la autenticación PassThrough con tarjeta inteligente en XenDesktop y XenApp para los usuarios de Citrix Receiver para Windows con dispositivos unidos a un dominio que no acceden a las tiendas a través de NetScaler Gateway, este parámetro se aplica a todos los usuarios de la tienda. Si desea habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear tiendas independientes para cada método de autenticación. Los usuarios deben conectarse a la tienda adecuada para su método de autenticación.

Si habilita la autenticación PassThrough con tarjeta inteligente en XenDesktop y XenApp para los usuarios de Citrix Receiver

para Windows con dispositivos unidos a un dominio que acceden a las tiendas a través de NetScaler Gateway, este parámetro se aplica a todos los usuarios de la tienda. Si desea habilitar la autenticación PassThrough para algunos usuarios y solicitar a otros usuarios que inicien sesión en los escritorios y aplicaciones, debe crear tiendas independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios a la tienda adecuada para su método de autenticación.

Uso de tarjetas inteligentes con Citrix Receiver para iOS y Android

Los usuarios con dispositivos que ejecutan Citrix Receiver para iOS y Citrix Receiver para Android se pueden autenticar con tarjetas inteligentes, ya sea directamente o a través de NetScaler Gateway. Se pueden usar los dispositivos que no pertenezcan a ningún dominio.



En el caso de dispositivos de la red local, los usuarios reciben como mínimo dos peticiones de credenciales. Cuando los usuarios se autentican en StoreFront o crean la tienda por primera vez, se les solicita el PIN de la tarjeta inteligente. Con la configuración apropiada, los usuarios tienen que volver a introducir su PIN solamente cuando acceden a sus escritorios y a sus aplicaciones. Para ello, habilite la autenticación con tarjeta inteligente en StoreFront e instale los controladores de tarjeta inteligente en el VDA.

Con estos Citrix Receivers, tiene la opción de especificar tarjetas inteligentes o credenciales de dominio. Si ha creado una tienda para usar tarjetas inteligentes y quiere conectarse a la misma tienda mediante credenciales de dominio, debe agregar una tienda independiente sin activar las tarjetas inteligentes.

Los usuarios que se conectan a través de NetScaler Gateway deben iniciar la sesión usando su tarjeta inteligente y su PIN al menos dos veces para acceder a sus escritorios y aplicaciones. Los usuarios se autentican usando su tarjeta inteligente y su PIN y, con la configuración apropiada, solo tienen que volver a introducir su PIN cuando acceden a sus escritorios y aplicaciones. Para conseguir esto, hay que habilitar la autenticación PassThrough con NetScaler Gateway en StoreFront y delegar la validación de credenciales en NetScaler Gateway. Después, cree un servidor virtual adicional de NetScaler Gateway a través del cual se enrutarán las conexiones de usuario hacia sus recursos.

Los usuarios pueden iniciar sesión en NetScaler Gateway con sus tarjetas inteligentes y sus PIN o con credenciales explícitas, según cómo haya especificado la autenticación de la conexión. Configure la autenticación PassThrough de NetScaler Gateway a StoreFront y delegue la validación de las credenciales a NetScaler Gateway para los usuarios de tarjeta inteligente de modo que los usuarios se autentiquen silenciosamente en StoreFront. Si quiere cambiar el método de autenticación, debe eliminar y volver a crear la conexión.

Uso de tarjetas inteligentes con Citrix Receiver para Linux

Los usuarios con dispositivos que ejecutan Citrix Receiver para Linux se pueden autenticar mediante tarjetas inteligentes de una forma similar a la de los usuarios de dispositivos que no pertenecen a un dominio de Windows. Incluso aunque el usuario se autentique en el dispositivo Linux con una tarjeta inteligente, Citrix Receiver para Linux no tiene ningún mecanismo para

adquirir ni reutilizar el PIN especificado.

Configure los componentes del lado del servidor para las tarjetas inteligentes de la misma forma que los configura para su uso con Citrix Receiver para Windows. Consulte How To Configure StoreFront 2.x and Smart Card Authentication for Internal Users using Stores y, para obtener instrucciones acerca del uso de tarjetas inteligentes, consulte Citrix Receiver para Linux.

La cantidad mínima de solicitudes de inicio de sesión que los usuarios pueden recibir es 1. Los usuarios inician sesión en sus dispositivos y, a continuación, se autentican en Citrix Receiver para Linux con sus tarjetas inteligentes y sus PIN. Los usuarios no tienen que volver a introducir su PIN cuando acceden a sus escritorios y a sus aplicaciones. Para conseguir esto, hay que habilitar la autenticación con tarjeta inteligente en StoreFront.

Como los usuarios inician sesión en Citrix Receiver para Linux directamente, puede permitir que estos recurran a la autenticación explícita. Si se configura tanto la autenticación explícita como la autenticación con tarjeta inteligente, primero se solicita a los usuarios que inicien sesión con sus tarjetas inteligentes y sus PIN. En caso de problemas con las tarjetas inteligentes, también tendrán la opción de seleccionar la autenticación explícita.

Los usuarios que se conectan a través de NetScaler Gateway deben iniciar la sesión usando su tarjeta inteligente y su PIN al menos una vez para acceder a sus escritorios y a sus aplicaciones. Los usuarios se autentican mediante su tarjeta inteligente y su PIN y, con la configuración apropiada, no tienen que volver a introducir su PIN cuando acceden a sus escritorios y a sus aplicaciones. Para conseguir esto, hay que habilitar la autenticación PassThrough con NetScaler Gateway en StoreFront y delegar la validación de credenciales en NetScaler Gateway. Después, cree un servidor virtual adicional de NetScaler Gateway a través del cual se enrutarán las conexiones de usuario hacia sus recursos.

Los usuarios pueden iniciar sesión en NetScaler Gateway con su tarjeta inteligente y su PIN o con credenciales explícitas. Esto permite ofrecer a los usuarios la opción de recurrir a la autenticación explícita para iniciar sesión con NetScaler Gateway. Configure la autenticación PassThrough de NetScaler Gateway a StoreFront y delegue la validación de las credenciales a NetScaler Gateway para los usuarios de tarjeta inteligente de modo que los usuarios se autentiquen silenciosamente en StoreFront.

Las tarjetas inteligentes para Citrix Receiver para Linux no están respaldadas en sitios de respaldo de servicios XenApp.

Una vez que el respaldo para tarjetas inteligentes está habilitado para el servidor y para Citrix Receiver, y si la directiva de aplicación de los certificados de tarjeta inteligente lo permite, puede utilizar tarjetas inteligentes con los siguientes fines:

- Autenticación de inicio de sesión con tarjetas inteligentes. Utilice tarjetas inteligentes para autenticar usuarios en servidores de Citrix XenApp y XenDesktop.
- Respaldo para aplicaciones de tarjetas inteligentes. Habilite las aplicaciones publicadas compatibles con tarjetas inteligentes para que puedan acceder a dispositivos de tarjetas inteligentes locales.

Uso de tarjetas inteligentes con la asistencia de los servicios XenApp

Los usuarios que inician sesión en los sitios de respaldo de servicios XenApp para iniciar aplicaciones y escritorios se pueden autenticar mediante tarjetas inteligentes sin depender de ningún hardware, sistema operativo o Citrix Receiver específico. Cuando un usuario accede a un sitio de respaldo de servicios XenApp e introduce correctamente una tarjeta inteligente y un PIN, PNA determina la identidad del usuario, lo autentica en StoreFront y devuelve los recursos disponibles.

Para que funcionen la autenticación PassThrough y la autenticación con tarjeta inteligente, debe habilitar la opción Confiar en las solicitudes enviadas a XML Service.

Utilice una cuenta con permisos de administrador local en el Delivery Controller para iniciar Windows PowerShell y, en el símbolo del sistema, escriba los siguientes comandos para permitir que el Delivery Controller confíe en las solicitudes XML enviadas desde StoreFront. El siguiente procedimiento se aplica a XenApp 7.5 - 7.8 y XenDesktop 7.0 - 7.8.

1. Cargue los cmdlets de Citrix escribiendo asnp Citrix*. (incluya el punto final).
2. Escriba **Add-PSSnapin citrix.broker.admin.v2**.
3. Escriba **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**
4. Cierre PowerShell.

Para obtener información sobre cómo configurar el respaldo para el método de autenticación con tarjeta inteligente de los servicios XenApp, consulte Configuración de la autenticación de las direcciones URL de servicios XenApp.

Consideraciones importantes

El uso de tarjetas inteligentes para la autenticación de usuarios con StoreFront está sujeto a los siguientes requisitos y restricciones.

- Para utilizar túneles VPN con la autenticación mediante tarjeta inteligente, los usuarios deben instalar NetScaler Gateway Plug-in e iniciar sesión a través de una página Web utilizando las tarjetas inteligentes y los PIN en cada paso de la autenticación. La autenticación PassThrough en StoreFront con NetScaler Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.
- Se pueden utilizar varias tarjetas inteligentes y varios lectores en el mismo dispositivo de usuario, pero si desea habilitar la autenticación PassThrough con tarjeta inteligente, los usuarios deben asegurarse de que haya solamente una tarjeta inteligente insertada durante el acceso a un escritorio o aplicación.
- Cuando se utiliza una tarjeta inteligente dentro de una aplicación (por ejemplo, para las funciones de cifrado o firma digital), es posible que se muestren solicitudes adicionales para insertar una tarjeta inteligente o introducir un PIN. Esto puede suceder cuando se inserta más de una tarjeta inteligente al mismo tiempo. También puede deberse a parámetros de configuración, tales como parámetros de middleware como el caché de PIN, que se configuran generalmente con directivas de grupo. Si los usuarios ven una solicitud donde se les pide que introduzcan la tarjeta inteligente cuando la tarjeta inteligente ya está en el lector, deben hacer clic en Cancelar. Si se solicita un PIN, los usuarios deben introducir de nuevo los PIN.
- Si habilita la autenticación PassThrough con tarjeta inteligente en XenDesktop y XenApp para los usuarios de Citrix Receiver para Windows con dispositivos unidos a un dominio que no acceden a las tiendas a través de NetScaler Gateway, este parámetro se aplica a todos los usuarios de la tienda. Si desea habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear tiendas independientes para cada método de autenticación. Los usuarios deben conectarse a la tienda adecuada para su método de autenticación.
- Si habilita la autenticación PassThrough con tarjeta inteligente en XenDesktop y XenApp para los usuarios de Citrix Receiver para Windows con dispositivos unidos a un dominio que acceden a las tiendas a través de NetScaler Gateway, este parámetro se aplica a todos los usuarios de la tienda. Si desea habilitar la autenticación PassThrough para algunos usuarios y solicitar a otros usuarios que inicien sesión en los escritorios y aplicaciones, debe crear tiendas independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios a la tienda adecuada para su método de autenticación.
- Solo se puede configurar un método de autenticación para cada dirección URL de servicios XenApp, y solo está disponible una dirección URL por tienda. Si desea habilitar otros tipos de autenticación (además de la autenticación con tarjeta inteligente), debe crear tiendas independientes, cada una de ellos con una URL de servicios XenApp, para cada método de autenticación. A continuación, debe dirigir a los usuarios a la tienda adecuada para su método de autenticación.

- Cuando se instala StoreFront, la configuración predeterminada de Microsoft Internet Information Services (IIS) solo requiere que se presenten certificados del cliente para conexiones HTTPS para la URL de autenticación de certificados del servicio de autenticación de StoreFront. IIS no solicita certificados del cliente para otras direcciones URL de StoreFront. Estas configuraciones le permiten ofrecer a los usuarios de tarjeta inteligente la opción de utilizar la autenticación explícita si tienen problemas con las tarjetas inteligentes. Según la configuración de las directivas de Windows, los usuarios también pueden quitar sus tarjetas inteligentes sin necesidad de volver a autenticarse.

  Si decide configurar IIS para solicitar certificados del cliente en caso de conexiones HTTPS a todas las direcciones URL de StoreFront, el servicio de autenticación y las tiendas deben colocarse en el mismo servidor. Debe usar un certificado del cliente válido para todas las tiendas. Con esta configuración de sitio de IIS, los usuarios de tarjetas inteligentes no pueden conectarse a través de NetScaler Gateway y no pueden utilizar la autenticación explícita. Los usuarios deben iniciar sesión de nuevo si quitan las tarjetas inteligentes de los dispositivos.

Mejora de la experiencia de usuario

Aug 14, 2017

StoreFront incluye funciones diseñadas para mejorar la experiencia de usuario. Estas funciones se configuran de forma predeterminada cuando se crean las nuevas tiendas y los correspondientes sitios de Citrix Receiver para Web, sitios de Desktop Appliance, y direcciones URL de servicios XenApp asociados.

Control del espacio de trabajo

Cuando los usuarios se mueven entre los dispositivos, el control del espacio de trabajo garantiza que las aplicaciones que están usando sigan disponibles. Los usuarios pueden seguir trabajando con las mismas instancias de aplicaciones a través de varios dispositivos, en lugar de tener que reiniciar sus aplicaciones cada vez que inician sesión en un nuevo dispositivo. Esto permite, por ejemplo, que los médicos en los hospitales ahorren tiempo mientras se mueven de una estación de trabajo a otra para acceder a datos de los pacientes.

El control del espacio de trabajo está habilitado de forma predeterminada para los sitios de Citrix Receiver para Web y las conexiones a las tiendas a través de las direcciones URL de servicios XenApp. Cuando los usuarios inician sesión, vuelven a conectarse automáticamente a las aplicaciones que dejaron en ejecución. Por ejemplo: piense en un usuario que inicia sesión en una tienda, ya sea mediante el sitio de Citrix Receiver para Web o la URL de servicios XenApp, e inicia algunas aplicaciones. Si, a continuación, el usuario inicia sesión en la misma tienda, con el mismo método de acceso, pero en otro dispositivo, las aplicaciones iniciadas se transfieren automáticamente al nuevo dispositivo. Todas las aplicaciones que el usuario inicia en una tienda específica se desconectan automáticamente (pero no se cierran) cuando el usuario cierra sesión en la tienda. En el caso de los sitios de Citrix Receiver para Web, se debe usar el mismo explorador para iniciar sesión, iniciar las aplicaciones y cerrar sesión.

El control del espacio de trabajo para las direcciones URL de servicios XenApp no se puede configurar ni inhabilitar. Para obtener más información acerca de la configuración del control del espacio de trabajo en los sitios de Citrix Receiver para Web, consulte Configuración del control del espacio de trabajo.

El uso del control del espacio de trabajo en el sitio de Citrix Receiver para Web está sujeto a los siguientes requisitos y limitaciones.

- El control del espacio de trabajo no está disponible cuando se accede a los sitios de Citrix Receiver para Web desde aplicaciones y escritorios alojados.
- Para los usuarios que acceden a los sitios de Citrix Receiver para Web desde dispositivos Windows, el control del espacio de trabajo solo se habilita si el sitio puede detectar que Citrix Receiver se encuentra instalado en los dispositivos de los usuarios, o bien, si se utiliza Citrix Receiver para HTML5 para acceder a los recursos.
- Para poder reconectarse a aplicaciones desconectadas, los usuarios que acceden a los sitios de Citrix Receiver para Web a través de Internet Explorer deben agregar el sitio a las zonas de Intranet local o Sitios de confianza.
- Si solo hay un escritorio disponible para el usuario de un sitio de Citrix Receiver para Web que está configurado con el objetivo de iniciar escritorios únicos automáticamente cuando el usuario inicia sesión, las aplicaciones de ese usuario no se vuelven a conectar, independientemente de la configuración del control del espacio de trabajo.
- Los usuarios deben desconectarse de las aplicaciones con el mismo explorador que utilizaron originalmente para iniciarlas. Los recursos que se iniciaron con otro explorador o que se iniciaron de forma local desde el escritorio o desde el menú Inicio mediante Citrix Receiver no pueden desconectarse ni cerrarse a través de sitios de Citrix Receiver para Web.

Redirección de contenido

Cuando los usuarios se han suscrito a la aplicación adecuada, la redirección de contenido hace que los archivos locales de los usuarios se abran mediante las aplicaciones suscritas. Para habilitar la redirección de archivos locales, asocie la aplicación con los tipos de archivo necesarios en XenDesktop o XenApp. La asociación de tipos de archivos está habilitada de forma predeterminada en las tiendas nuevas. Para obtener más información, consulte Inhabilitación de la asociación de tipos de archivo.

Cambios de contraseña por parte del usuario

Puede permitir que los usuarios de los sitios de Citrix Receiver para Web inicien sesión con credenciales de dominio de Microsoft Active Directory para cambiar sus contraseñas en cualquier momento. También puede restringir los cambios de contraseña a los usuarios cuyas contraseñas han caducado. De esta manera, los usuarios siempre podrán acceder a sus escritorios y aplicaciones, aunque su contraseña haya caducado.

Si permite que los usuarios de los sitios de Citrix Receiver para Web cambien sus contraseñas en cualquier momento, los usuarios locales cuyas contraseñas están a punto de caducar reciben una advertencia cuando inician sesión. De forma predeterminada, el período de notificación para un usuario se determina mediante la configuración de directiva de Windows correspondiente. Las advertencias de caducidad de contraseña solo se muestran a los usuarios que se conectan desde la red interna. Para obtener más información sobre cómo permitir a los usuarios cambiar sus contraseñas, consulte Configuración del servicio de autenticación.

Los usuarios que inician sesión en los sitios de Desktop Appliance solo pueden cambiar las contraseñas caducadas, incluso aunque esté permitido el cambio de contraseñas en cualquier momento. Los sitios de Desktop Appliance no proporcionan controles para permitir que los usuarios cambien sus contraseñas después de que hayan iniciado sesión.

Al crear el servicio de autenticación, la configuración predeterminada impide que los usuarios de los sitios de Citrix Receiver para Web cambien sus contraseñas, incluso aunque hayan caducado. Si decide habilitar esta función, asegúrese de que las directivas para los dominios que contengan los servidores no impidan a los usuarios cambiar sus contraseñas. StoreFront debe poder ponerse en contacto con el controlador de dominio para cambiar las contraseñas de los usuarios.

Cuando se permite a los usuarios que cambien sus contraseñas, funciones importantes de seguridad se dejan a merced de cualquier persona que pueda acceder a las tiendas mediante el servicio de autenticación. Si su organización cuenta con una directiva de seguridad que solo permite utilizar las funciones de cambio de contraseñas de los usuarios para uso interno, asegúrese de que no se pueda acceder a las tiendas desde fuera de la red corporativa.

Vistas de escritorios y aplicaciones del sitio de Citrix Receiver para Web

Cuando es posible acceder a escritorios y aplicaciones desde el sitio de Citrix Receiver para Web, el sitio muestra vistas separadas para los escritorios y las aplicaciones de forma predeterminada. Los usuarios ven la vista de escritorio primero al iniciar sesión en el sitio. Independientemente de si también hay aplicaciones disponibles en el sitio de Citrix Receiver para Web, si hay un solo escritorio disponible para el usuario, el sitio iniciará ese escritorio automáticamente cuando el usuario inicie una sesión. Puede configurar las vistas que se deben mostrar para los sitios y evitar que los sitios de Citrix Receiver para Web inicien automáticamente escritorios para los usuarios. Para obtener más información, consulte Configuración de la forma en que se muestran los recursos a los usuarios.

El comportamiento de las vistas de los sitios de Citrix Receiver para Web depende de los tipos de recursos que se entreguen. Por ejemplo: los usuarios deben suscribirse a las aplicaciones antes de que aparezcan en la vista de aplicación, mientras que todos los escritorios disponibles para un usuario se muestran automáticamente en la vista de escritorio. Por este motivo, los usuarios no pueden eliminar escritorios de la vista de escritorio y no pueden arrastrar y colocar los iconos para reorganizar los escritorios. Cuando el administrador de XenDesktop permite el reinicio de los escritorios, la vista de escritorio ofrece controles para que los usuarios puedan reiniciar los escritorios. Si los usuarios tienen acceso a varias instancias de un

escritorio desde un solo grupo de escritorios, los sitios de Citrix Receiver para Web agregan sufijos numéricos a los nombres de los escritorios para distinguir los escritorios de los usuarios.

Para los usuarios que se conectan a las tiendas a través de Citrix Receiver o las direcciones URL de servicios XenApp, el cliente Citrix determina la manera en que se muestran los escritorios, las aplicaciones y su comportamiento.

Recomendaciones adicionales

Al entregar aplicaciones con XenDesktop y XenApp, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios cuando acceden a sus aplicaciones a través de las tiendas. Para obtener más información acerca de la entrega de aplicaciones, consulte Crear una aplicación de grupo de entrega.

- Organice las aplicaciones en carpetas para facilitarles a los usuarios la búsqueda de lo que necesitan cuando examinen los recursos disponibles. Las carpetas que crea en XenDesktop y XenApp aparecerán como categorías en Citrix Receiver. Por ejemplo: puede agrupar las aplicaciones según su tipo o, de forma alternativa, puede crear carpetas para diferentes roles de usuario dentro de la organización.
- Asegúrese de poner descripciones pertinentes cuando entrega las aplicaciones, dado que estas descripciones estarán visibles para los usuarios de Citrix Receiver.
- Puede especificar que todos los usuarios tengan un conjunto básico de aplicaciones "obligatorias" que no se pueden quitar de la página de inicio de Citrix Receiver. Para ello, agregue la cadena KEYWORDS:Mandatory a la descripción de la aplicación si quiere que sea obligatoria. Los usuarios pueden seguir utilizando las opciones de autoservicio para agregar más aplicaciones o quitar las que no sean obligatorias.
- Puede suscribir automáticamente a todos los usuarios de una tienda a una aplicación. Para ello, agregue la cadena KEYWORDS:Auto a la descripción que proporcione al entregar la aplicación. Cuando los usuarios inicien sesión en la tienda, la aplicación se suministrará automáticamente, sin necesidad de que los usuarios tengan que suscribirse de forma manual a ella.
- Para suscribir automáticamente a todos los usuarios de una tienda a una aplicación Web o de software como servicio (SaaS) administrada por App Controller, marque la casilla App is available in Citrix Receiver to all users automatically (Aplicación automáticamente disponible en Receiver para todos los usuarios) al configurar los parámetros de la aplicación.
- Si quiere anunciar aplicaciones de XenDesktop o facilitar a los usuarios la búsqueda de las aplicaciones más utilizadas, enumérelas en la lista Destacadas en Citrix Receiver. Para ello, agregue la cadena KEYWORDS:Featured a la descripción de la aplicación.
  Nota: Cuando se agregan varias palabras clave, hay que separarlas con espacios; por ejemplo: KEYWORDS:Auto Featured.
- De forma predeterminada, los escritorios compartidos y alojados en XenDesktop y XenApp se tratan como los demás escritorios en los sitios de Citrix Receiver para Web. Para cambiar este comportamiento, agregue la cadena KEYWORDS:TreatAsApp a la descripción de los escritorios. El escritorio se mostrará en las vistas de aplicaciones de los sitios de Citrix Receiver para Web, en lugar de aparecer en las vistas de escritorios, y los usuarios tendrán que suscribirse al escritorio previamente para poder usarlo. Además, el escritorio no se iniciará automáticamente cuando el usuario inicie sesión en el sitio de Citrix Receiver para Web y no se accederá a él mediante Desktop Viewer, aunque el sitio se haya configurado para permitir esto con los demás escritorios.
- Para los usuarios de Windows, puede especificar la preferencia de utilizar la versión instalada localmente de una aplicación, en vez de su instancia entregada equivalente, en caso de que ambas estén disponibles. Para ello, agregue la cadena **KEYWORDS:prefer="application"** a la descripción de la aplicación. En este caso, application es una o varias palabras completas del nombre de la aplicación local, tal y como consta en el nombre del archivo de acceso directo, o la ruta absoluta, incluido el nombre del archivo ejecutable, a la aplicación local desde la carpeta \Start Menu. Cuando un usuario se suscribe a una aplicación con esta palabra clave, Citrix Receiver busca el nombre especificado o la ruta de acceso en el dispositivo de usuario para determinar si la aplicación ya está instalada localmente. Si encuentra la aplicación, Citrix Receiver suscribe al usuario a la aplicación entregada, pero no crea un acceso directo. Cuando el usuario

inicia la aplicación entregada desde Citrix Receiver, se ejecuta la instancia instalada localmente. Para obtener más información, consulte Configuración de la entrega de aplicaciones.

Configuración multisitio de alta disponibilidad para StoreFront

Aug 14, 2017

StoreFront incluye una serie de funciones que se combinan para habilitar el equilibrio de carga y la conmutación por error entre las implementaciones que proporcionan recursos a las tiendas. Para una mayor resistencia, también puede especificar implementaciones dedicadas de recuperación ante desastres. Estas funciones le permiten configurar las implementaciones de StoreFront distribuidas en varios sitios para proporcionar alta disponibilidad de tiendas. Para obtener más información, consulte Configuraciones de tienda multisitio con alta disponibilidad.

Agrupación de recursos

De forma predeterminada, StoreFront enumera todas las implementaciones que proporcionan escritorios y aplicaciones a una tienda y trata todos esos recursos de manera diferenciada. Esto significa que, si el mismo recurso está disponible en más de una implementación, los usuarios verán un icono para cada recurso. Esto puede ser confuso si los recursos tienen el mismo nombre. Al definir una configuración multisitio de alta disponibilidad, puede agrupar las implementaciones de XenDesktop y XenApp que entregan el mismo escritorio o aplicación. De esta manera, los recursos que son idénticos se pueden combinar de cara a los usuarios. Las implementaciones agrupadas no tienen por qué ser idénticas. Sin embargo, los recursos deben tener el mismo nombre y la misma ruta de acceso para cada servidor que se va a combinar.

Cuando un escritorio o aplicación están disponibles desde varias implementaciones de XenDesktop y XenApp configuradas para una tienda concreta, StoreFront combina todas las instancias de ese recurso y presenta a los usuarios un solo icono. Las aplicaciones de App Controller no se pueden combinar. Cuando un usuario inicia un recurso combinado, StoreFront determina la instancia más adecuada de ese recurso para el usuario. Esta determinación se realiza en función de la disponibilidad del servidor, de si el usuario ya tiene una sesión activa y del orden especificado en la configuración.

StoreFront supervisa de manera dinámica los servidores que no responden a las solicitudes porque están experimentando una sobrecarga o no están disponibles temporalmente. Los usuarios son dirigidos a instancias de recursos en otros servidores hasta que se restablezcan las comunicaciones. En los servidores que puedan proporcionar los recursos, StoreFront intenta volver a usar las sesiones existentes para entregar recursos adicionales. Si un usuario ya tiene una sesión activa en una implementación que también proporciona el recurso solicitado, StoreFront vuelve a utilizar la sesión si es compatible con ese recurso. Minimizar el número de sesiones de cada usuario reduce el tiempo necesario para iniciar aplicaciones o escritorios adicionales, y puede permitir un uso más eficaz de las licencias de productos.

Después de comprobar la disponibilidad y las sesiones de usuario existentes, StoreFront utiliza el orden especificado en la configuración para determinar la implementación a la que se conecta el usuario. Si hay más de una implementación equivalente disponible para el usuario, puede especificar que los usuarios se conecten o a la primera implementación disponible o, de forma aleatoria, a cualquier implementación de la lista. Si los usuarios se conectan a la primera implementación disponible, se minimiza el número de implementaciones en uso para el número actual de usuarios. En cambio, la conexión aleatoria de usuarios proporciona una distribución más equitativa de los usuarios por todas las implementaciones disponibles.

Puede anular la ordenación de implementación especificada para recursos individuales de XenDesktop y XenApp. De esta manera, podrá definir las implementaciones preferidas a las que se conectarán los usuarios cuando accedan a un escritorio o aplicación concretos. Esto le permite, por ejemplo, especificar que los usuarios se conecten preferiblemente a una implementación específicamente adaptada para entregar un escritorio o aplicación concretos, mientras que utiliza las

implementaciones restantes para otros recursos. Para ello, agregue la cadena KEYWORDS:Primary a la descripción de la aplicación o escritorio de la implementación preferida y KEYWORDS:Secondary al recurso en otras implementaciones. Cuando sea posible, los usuarios se conectarán a la implementación que proporcione el recurso principal, independientemente del orden de implementación especificado en la configuración. Los usuarios se conectan con implementaciones que suministran recursos secundarios cuando la implementación preferida no está disponible.

Asignar usuarios a los recursos

De forma predeterminada, los usuarios que acceden a un almacén ven una combinación de todos los recursos disponibles en todas las implementaciones configuradas para ese almacén. Para proporcionar diferentes recursos a diferentes usuarios, puede configurar tiendas independientes o incluso separar las implementaciones de StoreFront. Sin embargo, al definir una configuración multisitio de alta disponibilidad, puede proporcionar acceso a implementaciones específicas en función de la pertenencia de los usuarios a grupos de Active Directory. Esto le permite definir experiencias diferentes para grupos de usuarios diferentes con una única tienda.

Por ejemplo: puede agrupar los recursos comunes para todos los usuarios en una implementación, y las aplicaciones de finanzas para el departamento de Cuentas en otra implementación. En esta configuración, un usuario que no es miembro del grupo de usuarios de Cuentas ve solamente los recursos comunes cuando accede a la tienda. En cambio, un miembro del grupo de usuarios de Cuentas verá tanto los recursos comunes como las aplicaciones de finanzas.

También puede crear una implementación para usuarios avanzados que proporcione los mismos recursos que las demás implementaciones, pero con hardware más rápido y eficaz. Esto le permite ofrecer una experiencia mejorada a usuarios fundamentales de la empresa, como el equipo ejecutivo. Todos los usuarios verán los mismos escritorios y las mismas aplicaciones cuando inicien sesión en la tienda, pero los miembros del grupo de usuarios Ejecutivos se conectarán de forma preferente a los recursos proporcionados por la implementación de usuario avanzado.

Sincronización de las suscripciones

Si desea permitir que los usuarios accedan a las mismas aplicaciones desde tiendas similares que se encuentren en diferentes implementaciones de StoreFront, las suscripciones a aplicaciones de los usuarios deben estar sincronizadas entre los grupos de servidores. De lo contrario, es posible que los usuarios que se suscriban a una aplicación en la tienda de una implementación de StoreFront tengan que volver a suscribirse a la aplicación cuando inicien sesión en otro grupo de servidores. Para proporcionar una experiencia de usuario fluida cuando se trata de usuarios que se mueven entre más de una implementación de StoreFront, puede configurar una sincronización periódica de las suscripciones a aplicaciones de los usuarios entre tiendas de diferentes grupos de servidores. Elija entre sincronización regular en un intervalo específico de tiempo o sincronización programada para momentos concretos del día. Para obtener más información, consulte Configuración de la sincronización de suscripciones.

Recursos dedicados para la recuperación ante desastres

Puede definir implementaciones específicas de recuperación ante desastres. Estas implementaciones no se utilizarán a menos que todas las demás no estén disponibles. Por lo general, las implementaciones de recuperación ante desastres no se combinan con las implementaciones principales; proporcionan solo un subconjunto de los recursos que están disponibles de forma habitual, y es posible que ofrezcan una experiencia de usuario menos fluida que otras. Cuando se especifica que una implementación se va a usar para la recuperación ante desastres, esa implementación no se usa para el equilibrio de carga ni para la conmutación por errores. Los usuarios no pueden acceder a los escritorios y las aplicaciones proporcionados por las implementaciones de recuperación ante desastres a menos que todas las demás implementaciones para las que se configuran las implementaciones de recuperación ante desastres dejen de estar disponibles.

Cuando el acceso a cualquier otra implementación se restablezca, los usuarios no pueden iniciar más recursos de

recuperación ante desastres, incluso si ya están usando un recurso así. Los usuarios que ejecutan recursos de recuperación ante desastres no se desconectan de esos recursos cuando se restablece el acceso a otras implementaciones. Sin embargo, no pueden volver a iniciar recursos de recuperación ante desastres una vez que han salido de ellos. Del mismo modo, StoreFront no intenta volver a usar sesiones existentes con implementaciones de recuperación ante desastres si hay otras que han pasado a estar disponibles.

Enrutamiento óptimo de NetScaler Gateway

Si ha configurado distintos dispositivos NetScaler Gateway para las implementaciones, StoreFront le permite definir el dispositivo óptimo para el acceso de los usuarios a cada una de las implementaciones que proporcionan recursos para una tienda. Por ejemplo, si crea una tienda que combina los recursos de dos ubicaciones geográficas, cada una con un dispositivo NetScaler Gateway, los usuarios que se conectan a través del dispositivo de una ubicación pueden iniciar un escritorio o aplicación en la otra ubicación. Sin embargo, de forma predeterminada, la conexión al recurso se enruta a través del dispositivo al que el usuario se conectó originalmente y, por lo tanto, debe atravesar la WAN corporativa.

Para mejorar la experiencia de usuario y reducir el tráfico de red a través de la WAN, puede especificar el dispositivo NetScaler Gateway más adecuado para cada una de las implementaciones. Con esta configuración, las conexiones de los usuarios a los recursos se enrutan automáticamente a través del dispositivo local a la implementación que proporciona los recursos, independientemente de la ubicación del dispositivo que usa el usuario para acceder a la tienda.

El enrutamiento óptimo de NetScaler Gateway también se puede usar en casos especiales en los que es necesario que los usuarios locales de la red interna inicien sesión en NetScaler Gateway para el análisis del punto final. Con esta configuración, los usuarios se conectan a la tienda a través del dispositivo NetScaler Gateway, pero no es necesario enrutar la conexión al recurso a través del dispositivo porque el usuario está en la red interna. En este caso, debe habilitar el enrutamiento óptimo, pero no especifique un dispositivo para la implementación. De este modo, las conexiones de usuario a los escritorios y las aplicaciones se enrutan directamente y no a través de NetScaler Gateway. Tenga en cuenta que también debe configurar una dirección IP concreta para el servidor virtual interno del dispositivo NetScaler Gateway. Especifique además una baliza interna inaccesible para que Citrix Receiver siempre se conecte a NetScaler Gateway, independientemente de la ubicación de red de los usuarios.

Equilibrio de carga del servidor global de NetScaler Gateway

StoreFront admite las implementaciones de NetScaler Gateway configuradas para equilibrar la carga del servidor global con varios dispositivos configurados con un único FQDN. Para la autenticación de usuario y para enrutar las conexiones de usuario a través del dispositivo adecuado, StoreFront debe poder distinguir los dispositivos. Como el FQDN del dispositivo no se puede usar como un identificador exclusivo en una configuración de equilibrio de carga del servidor global, debe configurar StoreFront con una dirección IP exclusiva para cada uno de los dispositivos. Normalmente, esta es la dirección IP del servidor virtual de NetScaler Gateway.

Para obtener más información acerca del equilibrio de carga, consulte Equilibrio de carga con NetScaler.

Consideraciones importantes

Si opta por una configuración multisitio de alta disponibilidad para las tiendas, tenga en cuenta los siguientes requisitos y restricciones.

- Los escritorios y las aplicaciones deben tener el mismo nombre y la misma ruta de acceso en cada servidor para combinarse. Además, los recursos combinados, como los nombres y los iconos, deben tener las mismas propiedades. Si no, los usuarios podrían ver que las propiedades de los recursos cambian cuando Citrix Receiver enumera los recursos disponibles.

- Los escritorios asignados, tanto los preasignados como los que se asignan en el momento del primer uso, no deben combinarse. Asegúrese de que los grupos de entrega que suministran dichos escritorios no tienen el mismo nombre y la misma ruta en sitios configurados para la combinación.
- Las aplicaciones de App Controller no se pueden combinar.
- Si desea configurar la sincronización de las suscripciones a aplicaciones de los usuarios entre tiendas de diferentes implementaciones de StoreFront, las tiendas deben tener el mismo nombre en cada grupo de servidores. Además, ambos grupos de servidores deben residir en el dominio de Active Directory que contiene las cuentas de los usuarios o en un dominio que tenga una relación de confianza con el dominio de las cuentas de usuario.
- StoreFront solo proporciona acceso a copias de seguridad de las implementaciones de recuperación ante desastres cuando ninguno de los sitios principales del conjunto de implementaciones equivalentes está disponible. Si se comparte la copia de seguridad de una implementación entre varios conjuntos de implementaciones equivalentes, los usuarios accederán a los recursos de recuperación ante desastres solamente si todos los sitios principales de cada uno de los conjuntos dejan de estar disponibles.

Instalación, configuración, actualización y desinstalación

Aug 14, 2017

Antes de instalar y configurar

Para instalar y configurar StoreFront, siga estos pasos en el orden indicado:

1. Si quiere utilizar StoreFront para entregar recursos de XenDesktop y XenApp a los usuarios, compruebe que el servidor StoreFront está unido al dominio de Microsoft Active Directory que contiene las cuentas de los usuarios o a un dominio que tiene una relación de confianza con el dominio de las cuentas de usuario.

   Importante:
   - En implementaciones de servidor único puede instalar StoreFront en un servidor que no esté unido a un dominio.
   StoreFront no se puede instalar en un controlador de dominio.

2. Si aún no está instalado, StoreFront necesita Microsoft .NET 4.5 Framework, que se puede descargar desde Microsoft. Microsoft .NET 4.5 debe estar instalado antes de instalar StoreFront.
3. Si, además, piensa configurar una implementación de StoreFront con varios servidores, configure un entorno de equilibrio de carga para los servidores StoreFront.

   Para utilizar NetScaler para el equilibrio de carga, defina un servidor virtual como proxy de los servidores StoreFront. Para obtener más información sobre cómo configurar NetScaler para el equilibrio de carga, consulte Equilibrio de carga con NetScaler.

   1. Asegúrese de que el equilibrio de carga esté habilitado en el dispositivo NetScaler.
   2. Para cada servidor StoreFront, cree servicios de equilibrio de carga HTTP o TLS individuales, según sea adecuado, utilizando el tipo de monitor StoreFront.
   3. Configure los servicios para insertar la dirección IP del cliente en el encabezado X-Forwarded-For HTTP de solicitudes reenviadas a StoreFront, sobrescribiendo todas las directivas globales.

      StoreFront requiere direcciones IP de los usuarios para establecer conexiones con sus recursos.

   4. Cree un servidor virtual y enlace los servicios al servidor virtual.
   5. En el servidor virtual, configure la persistencia usando el método de inserción de cookies si tiene instalada la versión más reciente de los Citrix Receivers en todas las plataformas y no necesita dar respaldo a Android; de lo contrario, configure la persistencia en función de la dirección IP de origen.Asegúrese de que el tiempo de vida (TTL) es suficiente para permitir que los usuarios permanezcan conectados al servidor tanto tiempo como sea necesario.

      La persistencia garantiza que solo se realiza el equilibrio de carga en la conexión de usuario inicial y posteriormente se dirigen las solicitudes subsiguientes de ese usuario al mismo servidor StoreFront.

4. De manera opcional, puede habilitar las siguientes funciones.

   - Características de .NET Framework 4.5 > .NET Framework 4.5, ASP.NET 4.5

   Si lo desea, puede habilitar los siguientes roles y sus dependencias en el servidor StoreFront.

   - Servidor Web (IIS) > Servidor Web > Características HTTP comunes > Documento predeterminado, Errores HTTP, Contenido estático, Redirección HTTP
   - Servidor Web (IIS) > Servidor Web > Estado y diagnóstico > Registro HTTP
   - Servidor Web (IIS) > Servidor Web > Seguridad > Filtro de solicitudes, Autenticación de Windows
   - En servidores Windows Server 2012:

     Servidor Web (IIS) > Servidor Web > Desarrollo de aplicaciones > Extensibilidad de .NET 4.5, Inicialización de aplicaciones, ASP.NET 4.5, Extensiones ISAPI, Filtros ISAPI

     En servidores Windows Server 2008 R2:

     Servidor Web (IIS) > Servidor Web > Desarrollo de aplicaciones > Extensibilidad de .NET, Inicialización de aplicaciones, ASP.NET, Extensiones ISAPI, Filtros ISAPI

   - Servidor Web (IIS) > Herramientas de administración > Consola de administración de IIS, Scripts y herramientas de administración de IIS

   El instalador de StoreFront comprueba la habilitación de todas las funciones y los roles de servidor.

5. Instale StoreFront.

   Si quiere que el servidor forme parte de un grupo de servidores StoreFront, la ubicación de la instalación y los parámetros del sitio Web IIS, ruta física e ID de sitio, deben ser idénticos en todos los servidores del grupo.
6. De manera opcional, configure Microsoft Internet Information Services (IIS) para HTTPS si planea utilizar HTTPS para proteger la comunicación entre

StoreFront y los dispositivos de los usuarios.

Se necesita HTTPS para la autenticación con tarjeta inteligente. De forma predeterminada, Citrix Receiver requiere conexiones HTTPS con las tiendas. Puede cambiar de HTTP a HTTPS en cualquier momento que desee después de instalar StoreFront, siempre que tenga la configuración de IIS apropiada.

Para configurar IIS para HTTPS, utilice la consola del administrador de Internet Information Services (IIS) en el servidor StoreFront. De esta manera, se creará un certificado de servidor firmado por la entidad de certificación de dominio. A continuación, agregue un enlace HTTPS al sitio Web predeterminado. Para obtener más información acerca de la creación de un certificado de servidor en IIS, consulte http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate. Para obtener más información acerca de cómo agregar un enlace HTTPS a un sitio IIS, consulte http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding.

7. Asegúrese de que los firewalls y otros dispositivos de red permiten el acceso a los puertos TCP 80 o 443, según corresponda, desde dentro y fuera de la red corporativa. Además, asegúrese de que ni los firewalls ni otros dispositivos de la red interna bloqueen el tráfico a los puertos TCP no asignados.

   Al instalar StoreFront, se configura una regla del Firewall de Windows. Esta regla habilita el acceso al archivo ejecutable de StoreFront a través de un puerto TCP aleatorio seleccionado de los puertos no reservados. Este puerto se utiliza para comunicaciones entre los servidores StoreFront en un grupo de servidores.

8. Si va a usar varios sitios Web de Internet Information Services (IIS), después de crear los sitios en IIS, use el SDK de PowerShell para crear una implementación de StoreFront en cada uno de ellos. Para obtener más información, consulte Varios sitios Web de Internet Information Services (IIS).
   Nota: StoreFront inhabilita la consola de administración cuando detecta varios sitios y muestra un mensaje a tal efecto.

9. Utilice la consola de administración de Citrix StoreFront para configurar el servidor.

Instalación de StoreFront

> **Important**
>
> Para evitar posibles errores y la pérdida de datos durante la instalación de StoreFront, asegúrese de que todas las aplicaciones están cerradas y de que no hay otras tareas u operaciones ejecutándose en el sistema de destino.

1. Descargue el programa de instalación desde la página de descarga.
2. Inicie sesión en el servidor StoreFront con una cuenta con permisos de administrador local.
3. Asegúrese de que Microsoft .NET 4.5 Framework, requisito necesario, esté instalado en el servidor.
4. Busque el paquete de instalación, localice CitrixStoreFront-x64.exe y ejecute el archivo como administrador.
   Nota: En servidores Windows Server 2008 R2, es posible que aparezca un mensaje que indica que se va a habilitar la función .NET. Si aparece este mensaje, haga clic en Sí.
5. Lea y acepte el contrato de licencia. A continuación, haga clic en Siguiente.
6. Si aparece la página Revisar requisitos previos, haga clic en Siguiente.
7. En la página Listo para instalar, compruebe los requisitos previos y los componentes de StoreFront enumerados para la instalación y haga clic en Instalar.
   Antes de la instalación de los componentes, se habilitan los siguientes roles, si no están ya configurados en el servidor.

   - Servidor Web (IIS) > Servidor Web > Características HTTP comunes > Documento predeterminado, Errores HTTP, Contenido estático, Redirección HTTP
   - Servidor Web (IIS) > Servidor Web > Estado y diagnóstico > Registro HTTP
   - Servidor Web (IIS) > Servidor Web > Seguridad > Filtro de solicitudes, Autenticación de Windows
   - En servidores Windows Server 2012:

     Servidor Web (IIS) > Servidor Web > Desarrollo de aplicaciones > Extensibilidad de .NET 4.5, Inicialización de aplicaciones, ASP.NET 4.5, Extensiones ISAPI, Filtros ISAPI

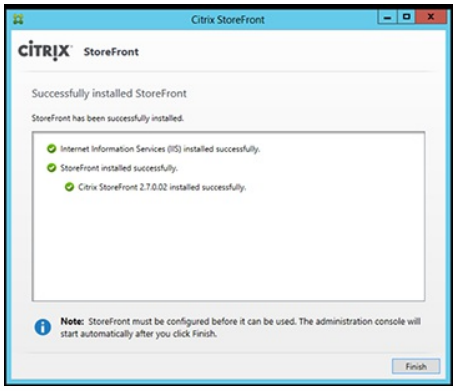
     En servidores Windows Server 2008 R2:

     Servidor Web (IIS) > Servidor Web > Desarrollo de aplicaciones > Extensibilidad de .NET, Inicialización de aplicaciones, ASP.NET, Extensiones ISAPI, Filtros ISAPI

   - Servidor Web (IIS) > Herramientas de administración > Consola de administración de IIS, Scripts y herramientas de administración de IIS

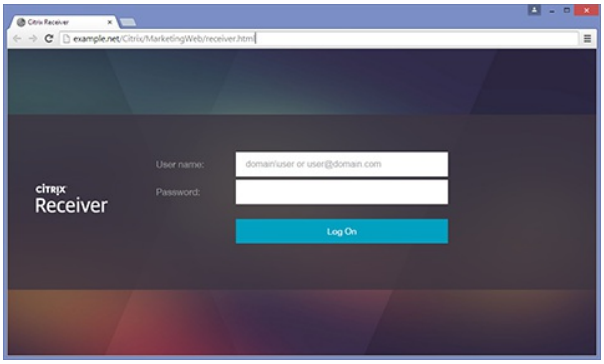
   Si no están ya configuradas, también se habilitan las siguientes funciones.

   - Características de .NET Framework 4.5 > .NET Framework 4.5, ASP.NET 4.5
8. Cuando termine la instalación, haga clic en Finalizar. La consola de administración de Citrix StoreFront se inicia automáticamente. También puede abrir StoreFront desde la pantalla Inicio.



9. En la consola de administración de Citrix StoreFront, haga clic en Crear una nueva implementación.
   1. Especifique la URL del servidor StoreFront en el cuadro **URL base**.
   2. En la página **Nombre de la tienda**, especifique un nombre para la tienda y haga clic en Siguiente.
10. En la página **Delivery Controllers**, enumere la infraestructura (datos detallados de los servicios de XenApp o XenDesktop) que proporciona los recursos que desea que estén disponibles en la tienda. Puede especificar un servidor "ficticio"; sin embargo, las aplicaciones no se mostrarán en la tienda.
11. Establezca el **Tipo de transporte** y el **Puerto.**Puede especificar HTTP y el puerto 443 y, a continuación, haga clic en **Aceptar**. También puede copiar la configuración de una implementación existente de Interfaz Web o StoreFront.
12. En la página **Acceso remoto**, seccione Ninguno. Si utiliza NetScaler Gateway, seleccione Sin túnel VPN e introduzca datos de su puerta de enlace.
13. En la página **Acceso remoto**, seccione Crear. Después de haber creado la tienda, haga clic en Finalizar.

Ahora, la tienda está disponible para que los usuarios accedan a ella mediante el sitio de Citrix Receiver para Web, lo que permite que los usuarios accedan a sus escritorios y aplicaciones a través de una página Web.
Aparecerá la dirección URL para que los usuarios accedan al sitio de Citrix Receiver para Web para la nueva tienda. Por ejemplo: example.net/Citrix/MarketingWeb/. Inicie sesión y accederá a la nueva interfaz de usuario de Citrix Receiver.



CEIP

Si se participa en el programa CEIP de mejora de la experiencia del usuario (Customer Experience Improvement Program), se envían estadísticas e información de uso anónimos a Citrix para mejorar la calidad y el rendimiento de sus productos.

De forma predeterminada, se inscribe automáticamente en el programa CEIP cuando instala StoreFront. La primera carga de datos tiene lugar aproximadamente siete días después de instalar StoreFront. Puede cambiar esta opción predeterminada en el parámetro de Registro del sistema. Si cambia el parámetro de Registro del sistema antes de instalar StoreFront, se usará ese valor. Si cambia el parámetro de Registro del sistema antes de actualizar StoreFront, se usará ese valor.

> ### Advertencia
>
> Si edita el Registro de forma incorrecta pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Debe hacer una copia de seguridad del Registro antes de editarlo.

El parámetro de Registro que controla la carga automática de los datos de análisis (predeterminado = 1):

Ubicación: HKLM:\Software\Citrix\Telemetry\CEIP

Nombre: Enabled

Tipo: REG_DWORD

Valor: 0 = inhabilitado, 1 = habilitado

De forma predeterminada, la propiedad "Enabled" está oculta en el Registro del sistema. Si no se especifica, significa que la funcionalidad de carga automática está habilitada.

Con PowerShell, el cmdlet siguiente inhabilita la inscripción en el programa CEIP:

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

Nota: El parámetro de Registro controla la carga automática de información anónima de uso y estadísticas para todos los componentes en el mismo servidor. Por ejemplo, si ha instalado StoreFront en el mismo servidor que el Delivery Controller y decide no participar en el programa CEIP usando el parámetro de Registro, la no participación se aplicará a ambos componentes.

Datos de CEIP recopilados desde StoreFront

La siguiente tabla ofrece ejemplos del tipo de información anónima que se recopila. Los datos no contienen detalles que lo identifiquen a usted como cliente.

Datos	Descripción
Versión de StoreFront	Cadena que indica la versión instalada de StoreFront. Por ejemplo, "3.8.0.0"
Recuento de tiendas	Un contador del número de tiendas que hay en la implementación.
Recuento de servidores en el grupo de servidores	Un contador del número de servidores del grupo de servidores.
Recuento de Delivery Controllers por tienda	Lista de valores numéricos que indican la cantidad Delivery Controllers disponibles para cada tienda en la implementación.
HTTPS habilitado	Cadena que indica si https está habilitado para la implementación. "True" o "False".
Experiencia clásica habilitada para Citrix Receiver	Lista de valores booleanos que indica si la "Experiencia clásica" está habilitada para cada Receiver para Web. TRUE o FALSE cada para Receiver para Web.
Parámetro HTML5 de Citrix Receiver	Lista de las cadenas de texto que indican el parámetro de HTML5 de Receiver para cada Receiver para Web. "Always","Fallback","Off" para cada Receiver para Web.
Control del espacio de trabajo habilitado para Citrix Receiver	Lista de valores booleanos que indican si el "Control del espacio de trabajo" está habilitado para cada Receiver para Web. TRUE o FALSE cada para Receiver para Web.
Acceso remoto habilitado en la tienda	Lista de las cadenas de texto que indican si el "Acceso remoto" está habilitado para cada tienda en la implementación. "ENABLED" o "DISABLED" para cada tienda.
Recuento de puertas de enlace	Un contador de la cantidad de puertas de enlace NetScaler Gateway configuradas en la implementación.

Para instalar StoreFront en un símbolo del sistema

1. Inicie sesión en el servidor StoreFront con una cuenta con permisos de administrador local.
2. Antes de instalar StoreFront, asegúrese de cumplir todos los requisitos para ello. Para obtener información más detallada, consulte Antes de instalar y configurar.
3. En los medios de instalación o el paquete de descarga, busque CitrixStoreFront-x64.exe y copie el archivo a una ubicación temporal en el servidor.
4. En un símbolo del sistema, vaya a la carpeta que contiene el archivo de instalación y escriba el siguiente comando.
   CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation] [-WINDOWS_CLIENT filelocation\filename.exe] [-MAC_CLIENT filelocation\filename.dmg]
   Utilice el argumento -silent para realizar una instalación silenciosa de StoreFront y de todos los requisitos previos. De forma predeterminada, StoreFront se instala en C:\Archivos de programa\Citrix\Receiver StoreFront\. No obstante, puede especificar otra ubicación de instalación con el argumento -INSTALLDIR, donde installationlocation es el directorio donde se instalará StoreFront. Si quiere que el servidor forme parte de un grupo de servidores StoreFront, la

ubicación de la instalación y los parámetros del sitio Web IIS, ruta física e ID de sitio, deben ser idénticos en todos los servidores del grupo.

De forma predeterminada, si un sitio de Citrix Receiver para Web no puede detectar Citrix Receiver en un dispositivo Windows o Mac OS X, se solicitará al usuario que descargue e instale la versión de Citrix Receiver correspondiente a su plataforma desde el sitio Web de Citrix. Puede modificar este comportamiento para que los usuarios descarguen los archivos de instalación de Citrix Receiver desde el servidor StoreFront. Para obtener más información, consulte Cómo ofrecer archivos de instalación de Citrix Receiver en el servidor.

Si va a realizar este cambio de configuración, especifique los argumentos -WINDOWS_CLIENT y -MAC_CLIENT para copiar, respectivamente, los archivos de instalación de Citrix Receiver para Windows y Citrix Receiver para Mac a la ubicación correspondiente de su implementación de StoreFront. Reemplace filelocation por el directorio que contiene el archivo de instalación a copiar y filename por el nombre del archivo de instalación de Citrix Receiver. Los archivos de instalación de Citrix Receiver para Windows y Citrix Receiver para Mac están incluidos en los medios de instalación o el paquete de descarga de StoreFront.

Actualización de StoreFront

Para actualizar implementaciones existentes de cualquier versión de StoreFront entre 2.0 y 3.0.x a esta versión de StoreFront, ejecute el archivo de instalación de esta versión de StoreFront. Las versiones anteriores a StoreFront 2.0 no se pueden actualizar directamente. En su lugar, primero hay que actualizar desde StoreFront 1.2 a StoreFront 2.0 y después actualizar a esta versión de StoreFront. De manera similar, no se puede actualizar StoreFront 1.1 directamente a esta versión de StoreFront. Primero es necesario actualizar el software desde StoreFront 1.1 a StoreFront 1.2 y desde ahí a StoreFront 2.0, para finalmente actualizar a esta versión de StoreFront.

Una vez iniciado el proceso de actualización, éste no puede deshacerse. Si la actualización se interrumpe o no se puede completar, la configuración existente se eliminará, pero StoreFront no se instalará. Antes de comenzar una actualización, es necesario desconectar a los usuarios de la implementación de StoreFront e impedir que accedan a los servidores mientras la actualización está teniendo lugar. De esta manera, el instalador puede acceder a todos los archivos de StoreFront durante la actualización. Si el instalador no pudiera acceder a alguno de los archivos, no se podrán reemplazar y, por lo tanto, la actualización no se podrá llevar a cabo, lo cual provocará la eliminación de la configuración existente de StoreFront. StoreFront no respalda implementaciones con varios servidores que contengan versiones diferentes del producto, por lo que todos los servidores de un grupo deben cambiar simultáneamente a la versión actualizada antes de conceder el acceso a la implementación. No se respalda la actualización simultánea para las implementaciones con varios servidores; los servidores deben actualizarse de forma secuencial. Citrix recomienda que realice una copia de seguridad de los datos antes de realizar la actualización.

Con la desinstalación de StoreFront se eliminan el servicio de autenticación, las tiendas, las suscripciones de usuarios a aplicaciones, los sitios de Citrix Receiver para Web, los sitios de Desktop Appliance, y las direcciones URL de servicios XenApp. Esto significa que, si decide desinstalar StoreFront, debe volver a crear manualmente los servicios, las tiendas y los sitios cuando vuelva a instalar StoreFront. La actualización también permite conservar la configuración de StoreFront y dejar los datos de suscripción a aplicaciones de los usuarios intactos, de modo que los usuarios no tengan que volver a suscribirse a todas sus aplicaciones.

La actualización de la versión de sistema operativo en un servidor que ejecuta StoreFront no está respaldada. Citrix recomienda instalar StoreFront en una instalación limpia del sistema operativo.

> **Important**
>
> Antes de iniciar la actualización:
>
> - Cierre todas las demás aplicaciones en el servidor StoreFront.
> - Cierre todas las líneas de comandos y ventanas de PowerShell.

Para actualizar desde StoreFront 2.0 - 3.0.x a esta versión de StoreFront

1. Inhabilite el acceso a la implementación a través del entorno de equilibrio de carga. Al inhabilitar la URL de equilibrio de carga, se impide que los usuarios se conecten a la implementación durante la actualización.
2. Haga una copia de respaldo de todos los servidores del grupo.
3. Quite uno de los servidores del grupo de servidores existente.
4. Reinicie el servidor que ha quitado.
   Tenga en cuenta que puede utilizar un equilibrador de carga paralelo para comprobar el buen funcionamiento del nuevo grupo de servidores a medida que lo construye. La manera de proceder que aumenta al máximo la disponibilidad e implica el mínimo riesgo consiste en quitar y actualizar solo un servidor del grupo de servidores original. De esa manera, se puede construir literalmente el nuevo grupo de servidores a partir de máquinas nuevas, en lugar de utilizar para ello las máquinas que se han quitado del grupo de servidores original.
5. Actualice el servidor que ha quitado con una cuenta de administrador. Este proceso no debe realizarse a la par que se ejecutan instalaciones en el servidor, solo deberían estar en ejecución las aplicaciones mínimas.
6. Compruebe que el servidor que ha quitado se ha actualizado correctamente.
7. Quite, del equilibrador de carga, otro de los servidores que compone el grupo existente.

8. Reinicie el servidor que ha quitado por las mismas razones que las explicadas en el paso 1.
9. Desinstale la versión actualmente instalada de StoreFront e instale la nueva versión de StoreFront.
10. Una el servidor recién instalado a un grupo de servidores nuevo, compuesto de todos los servidores actualizados y los servidores recién instalados. Compruebe que funcionan correctamente.
11. Repita los pasos del 3 al 10 hasta que el grupo de servidores nuevo tenga la capacidad suficiente como para asumir las funciones del grupo de servidores anterior. Apunte el equilibrador de carga al nuevo grupo de servidores y compruebe que funciona correctamente.
12. Repita los pasos del 3 al 10 para los servidores restantes; agregue cada uno al equilibrador de carga a medida que se vayan actualizando correctamente.

> **Nota**
>
> - Si quiere una disponibilidad máxima, puede mantener el acceso al grupo original de servidores durante el proceso de actualización hasta que el grupo nuevo esté disponible. Para ello:
>   1. Omita el paso 1.
>   2. Modifique el paso 11 para incluir la inhabilitación del acceso al grupo de servidores original mediante el equilibrador de carga. Exporte los datos de suscripción del grupo de servidores original e impórtelos al nuevo grupo de servidores. Habilite el acceso al nuevo grupo de servidores mediante el equilibrador de carga.
>
>   Con ello, todos los cambios de suscripción que los usuarios hayan realizado entre los pasos 3 y 11 estarán disponibles en el nuevo grupo de servidores.
> - Puede maximizar aún más la disponibilidad si quita solo un servidor del grupo de servidores original y lo actualiza; luego construye el nuevo grupo de servidores a partir de servidores nuevos, en vez de utilizar los servidores que quite del grupo de servidores original. Cuando el nuevo grupo de servidores esté en producción, podrá retirar los servidores antiguos.
> - Cuando se actualiza desde StoreFront 2.x a 3.x y luego se propaga el cambio al grupo de servidores, puede añadirse una entrada para pnaAuthenticationStartupModule en el archivo de configuración de la autenticación. Puesto que las entradas solo se pueden agregar a servicios de autenticación que han sido habilitados para servicios de autenticación de PNA y cambio de contraseña de PNA, el servicio de autenticación no puede iniciarse ya que le falta el modulo de inicio indicado. Solución temporal: Quite la entrada del archivo de configuración de autenticación. De manera predeterminada, el archivo de configuración se encuentra en C:\inetpub\wwwroot\Citrix\\web.config.

Configuración de StoreFront

Cuando la consola de administración de Citrix StoreFront se inicia por primera vez, existen dos opciones disponibles.

- Crear una nueva implementación. Configure el primer servidor de una nueva implementación de StoreFront. Las implementaciones de un servidor único son idóneas para la evaluación de StoreFront o para implementaciones pequeñas de producción. Después de configurar el primer servidor StoreFront, puede agregar más servidores al grupo en cualquier momento para aumentar la capacidad de la implementación.
- Incorporarse a un grupo de servidores existente.Agregue otro servidor a una implementación existente de StoreFront. Seleccione esta opción para aumentar rápidamente la capacidad de la implementación de StoreFront. Se necesita equilibrio de carga externo para las implementaciones con varios servidores. Para agregar un nuevo servidor, necesitará acceso a un servidor existente de la implementación.

Desinstalación de StoreFront

Además del producto en sí, la desinstalación de StoreFront conlleva la eliminación del servicio de autenticación, las tiendas, los sitios de Citrix Receiver para Web, los sitios de Desktop Appliance, las direcciones URL de servicios XenApp y sus configuraciones asociadas. El servicio de tiendas de suscripción que contiene los datos de suscripción a aplicaciones de los usuarios también se elimina. En implementaciones de un solo servidor, esto significa que la información sobre suscripciones a aplicaciones de los usuarios se pierde. No obstante, en implementaciones de varios servidores, estos datos se conservan en otros servidores del grupo. Los requisitos previos habilitados por el instalador de StoreFront, como las funciones de .NET Framework y los servicios de rol de Servidor web (IIS), no se eliminan del servidor cuando se desinstala StoreFront.

1. Inicie sesión en el servidor StoreFront con una cuenta con permisos de administrador local.
2. En la pantalla **Inicio** o Aplicaciones de Windows, busque el icono de **Citrix StoreFront** y haga clic en él. Haga clic con el botón secundario en el icono y haga clic en **Desinstalar**.
3. En el cuadro de diálogo **Programas y características**, seleccione **Citrix StoreFront** y haga clic en **Desinstalar** para eliminar todos los componentes de StoreFront del servidor.
4. En el cuadro de diálogo **Desinstalar Citrix StoreFront**, haga clic en **Sí**. Cuando termine la desinstalación, haga clic en **Aceptar**.

Creación de una nueva implementación

Aug 14, 2017

1. Si la consola de administración de Citrix StoreFront aún no está abierta después de la instalación de StoreFront, haga clic en la pantalla Inicio o Aplicaciones de Windows y haga clic en el icono Citrix StoreFront.
2. En el panel de resultados de la consola de administración de Citrix StoreFront, haga clic en Crear una nueva implementación.
3. Especifique la URL del servidor StoreFront o el entorno de equilibrio de carga (si se trata de una implementación con varios servidores) en el cuadro URL base.
   Si aún no ha configurado el entorno de equilibrio de carga, especifique la URL del servidor. Puede modificar la URL base de la implementación en cualquier momento.

   Puede cambiar de HTTP a HTTPS en cualquier momento con la tarea Cambiar URL base de la consola de administración de StoreFront, siempre que Microsoft Internet Information Services (IIS) esté configurado para HTTPS.

4. Haga clic en Siguiente para configurar el servicio de autenticación, que autentica a los usuarios en Microsoft Active Directory.
   Para utilizar HTTPS para proteger la comunicación entre StoreFront y los dispositivos de los usuarios, debe configurar Microsoft Internet Information Services (IIS) para HTTPS. Sin una configuración de IIS adecuada, StoreFront utiliza HTTP para las comunicaciones.

   De forma predeterminada, Citrix Receiver requiere conexiones HTTPS con las tiendas. Si StoreFront no está configurado para HTTPS, los usuarios deben llevar a cabo pasos de configuración adicionales para usar conexiones HTTP. Se necesita HTTPS para la autenticación con tarjeta inteligente. Puede cambiar de HTTP a HTTPS en cualquier momento que desee después de configurar StoreFront, siempre que tenga la configuración de IIS apropiada. Para obtener más información, consulte Configuración de grupos de servidores.

   Puede cambiar de HTTP a HTTPS en cualquier momento con la tarea **Cambiar URL base** de la consola de administración de StoreFront, siempre que Microsoft Internet Information Services (IIS) esté configurado para HTTPS.

5. En la página Nombre de la tienda, especifique un nombre para la tienda y si desea permitir solo acceso a usuarios no autenticados (anónimos) y haga clic en Siguiente.
   Las tiendas de StoreFront combinan escritorios y aplicaciones, y los ponen a disposición de los usuarios. Los nombres de las tiendas aparecen en Citrix Receiver en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido de la tienda.

6. En la página Controllers, busque la infraestructura que proporciona los recursos que desea que estén disponibles en la tienda. Para agregar escritorios y aplicaciones a la tienda, lleve a cabo el siguiente procedimiento. Puede configurar las tiendas para proporcionar recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y XenMobile (App Controller). Repita los procedimientos tantas veces como sea necesario para agregar todas las implementaciones que proporcionan recursos a la tienda.
   - Cómo agregar recursos de XenDesktop y XenApp a la tienda
   - Cómo agregar aplicaciones de App Controller a la tienda
7. Una vez que haya agregado a la tienda todos los recursos necesarios, en la página Controllers, haga clic en Siguiente.
8. En la página Acceso remoto, especifique si los usuarios que se conectan desde redes públicas pueden acceder a los recursos internos, y cómo pueden hacerlo.
   - Para que la tienda esté disponible para los usuarios de redes públicas, marque la casilla **Habilitar acceso remoto**. Si

deja esta casilla sin marcar, solo los usuarios locales de la red interna podrán acceder a la tienda.

- Para hacer que solo los recursos entregados a través de la tienda estén disponibles a través de NetScaler Gateway, seleccione **Permitir a los usuarios acceder solo a los recursos entregados mediante StoreFront (sin túnel VPN)**.
- Para que la tienda y todos los demás recursos de la red interna estén disponibles a través del túnel de red privada virtual (VPN) de SSL (Secure Sockets Layer), seleccione **Permitir a los usuarios acceder a todos los recursos de la red interna (Túnel VPN completo).** Los usuarios necesitan el NetScaler Gateway Plug-in para establecer el túnel VPN.

Si configura el acceso remoto a la tienda a través de NetScaler Gateway, el método de autenticación PassThrough desde NetScaler Gateway se habilita automáticamente. Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.

9. Si ha habilitado el acceso remoto, enumere las implementaciones de NetScaler Gateway a través de las cuales los usuarios pueden acceder a la tienda. Para agregar una implementación de NetScaler Gateway, lleve a cabo el siguiente procedimiento. Repita los procedimientos tantas veces como sea necesario para agregar más implementaciones.
   - Cómo proporcionar acceso remoto a la tienda a través de un dispositivo NetScaler Gateway
   - Cómo proporcionar acceso remoto a la tienda a través de un clúster de Access Gateway 5.0
10. Una vez que haya agregado todas las implementaciones de NetScaler Gateway, seleccione de la lista de dispositivos NetScaler Gateway las implementaciones a través de las que los usuarios pueden acceder a la tienda. Si habilita el acceso a través de varias implementaciones, especifique la implementación predeterminada que se utilizará para acceder a la tienda.Haga clic en **Siguiente**.
11. En la página **Métodos de autenticación**, seleccione los métodos que los usuarios usarán para autenticarse en la tienda y haga clic en **Siguiente**. Se puede seleccionar uno de los siguientes métodos:

- **Nombre de usuario y contraseña:** Los usuarios deben introducir sus credenciales y autenticarse cuando acceden a las tiendas.
- **Autenticación SAML:** Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.
- **PassThrough de dominio:** Los usuarios se autentican en equipos Windows que están unidos a un dominio y sus credenciales se usan para iniciar sesión automáticamente cuando acceden a las tiendas.
- **Tarjeta inteligente:** Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a las tiendas.
- **HTTP básica:** Los usuarios se autentican con el servidor Web IIS del servidor StoreFront.
- **PassThrough desde NetScaler Gateway:** Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas. Esto se selecciona automáticamente cuando se habilita el acceso remoto.

12. En la página **URL de servicios XenApp**, configure la dirección URL de servicios XenApp para los usuarios que usen PNAgent para acceder a las aplicaciones y los escritorios.

13. Después de crear la tienda, se habilitan opciones adicionales en la consola de administración de Citrix StoreFront. Para obtener más información, consulte los artículos de administración.

La tienda está ahora disponible para que los usuarios accedan a él mediante Citrix Receiver, el cual debe estar configurado con los datos de acceso a la tienda. Existen diversas maneras de proporcionar esta información a los usuarios y facilitares el proceso de configuración. Para obtener más información, consulte Opciones de acceso de usuarios.

De manera alternativa, los usuarios pueden acceder a la tienda a través del sitio de Citrix Receiver para Web, que permite que los usuarios accedan a sus escritorios y aplicaciones a través de una página Web. La URL de acceso a un sitio de Citrix Receiver para Web, utilizada para acceder a la nueva tienda, aparece al crearla.

Al crear una nueva tienda, la URL de servicios XenApp correspondiente se habilita de forma predeterminada. Los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados que ejecuten el Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a las tiendas directamente mediante la URL de servicios XenApp para la tienda. La URL de los servicios XenApp tiene el formato http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, donde serveraddress es el nombre completo de dominio del servidor o del entorno de equilibrio de carga de la implementación de StoreFront y storename es el nombre especificado para la tienda cuando se creó en el paso 5.

Puede agregar rápidamente más servidores a la implementación mediante la selección de la opción Incorporarse a un grupo de servidores existente al instalar nuevas instancias de StoreFront.

Cómo agregar recursos de XenDesktop y XenApp a la tienda

Complete los siguientes pasos para que los escritorios y las aplicaciones que proporcionan XenApp y XenDesktop estén disponibles en la tienda que usted crea como parte de la configuración inicial del servidor StoreFront. Se presupone que usted ha completado los pasos 1 - 6 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

1. En la página Controllers del asistente Crear tienda en la consola de StoreFront, haga clic en Agregar.
2. En el cuadro de diálogo Agregar Delivery Controller, especifique un nombre que le ayude a identificar la implementación e indique si XenDesktop, XenApp o XenMobile proporcionan los recursos que desea poner en la tienda.
3. Agregue los nombres o las direcciones IP de los servidores a la lista Servidores. Especifique varios servidores para habilitar la tolerancia de fallos; para ello, enumere las entradas por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para los sitios de XenDesktop, proporcione información de los Controllers. En el caso de las comunidades de XenApp, enumere los servidores que ejecutan Citrix XML Service.
4. En la lista Tipo de transporte, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione HTTP. Si selecciona esta opción, deberá definir su propia configuración para proteger las conexiones entre StoreFront y los servidores.
   - Para enviar datos a través de conexiones HTTP seguras mediante SSL (Secure Sockets Layer) o TLS (Transport Layer Security), seleccione HTTPS. Si selecciona esta opción para servidores de XenDesktop y XenApp, asegúrese de que Citrix XML Service esté configurado para compartir su puerto con Microsoft Internet Information Services (IIS) y que IIS esté configurado para admitir HTTPS.
   - Para enviar datos a través de conexiones seguras a servidores XenApp y utilizar el Traspaso SSL para realizar la autenticación del host y el cifrado de datos, seleccione Traspaso SSL.

   Nota: Si utiliza HTTPS o el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres de servidores que especificó en la lista Servidores coincidan exactamente (incluidas mayúsculas y minúsculas) con los nombres en los certificados para esos servidores.
5. Especifique el puerto que StoreFront debe utilizar para las conexiones con los servidores. El puerto predeterminado para las conexiones que utilizan HTTP y el Traspaso SSL es 80, y para las conexiones mediante HTTPS es 443. En el caso de los servidores de XenDesktop y XenApp, el puerto especificado debe ser el puerto usado por Citrix XML Service.
6. Si utiliza el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores de XenApp, especifique el puerto TCP del Traspaso SSL en el cuadro Puerto del Traspaso SSL. El puerto predeterminado es 443. Asegúrese de que todos los servidores que ejecutan el Traspaso SSL estén configurados para escuchar en el mismo puerto.

Puede configurar las tiendas para proporcionar recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y XenMobile. Para agregar más sitios de XenDesktop o comunidades XenApp, repita el procedimiento anterior. Para que las aplicaciones que administra App Controller estén disponibles en la tienda, siga los pasos descritos en Cómo agregar

aplicaciones de App Controller a la tienda. Después de agregar todos los recursos necesarios a la tienda, vuelva al paso 7 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

Cómo agregar aplicaciones de App Controller a la tienda

Complete los siguientes pasos para que las aplicaciones administradas por App Controller estén disponibles en la tienda que usted cree como parte de la configuración inicial del servidor StoreFront. Se presupone que usted ha completado los pasos 1 - 6 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

1. En la página Delivery Controllers del asistente Crear tienda, haga clic en Agregar.
2. En el cuadro de diálogo Agregar Delivery Controller, especifique un nombre que lo ayude a identificar el dispositivo virtual App Controller que administra las aplicaciones que desea poner en la tienda. Asegúrese de que el nombre no contiene espacios. Seleccione AppController.
3. Escriba el nombre o la dirección IP del dispositivo virtual App Controller en el cuadro Servidor y especifique el puerto que StoreFront debe utilizar para las conexiones con App Controller. El puerto predeterminado es 443.

Puede configurar las tiendas para que proporcionen recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y App Controller. Para agregar aplicaciones administradas por otros dispositivos virtuales App Controller, repita el procedimiento anterior. Para que los escritorios y las aplicaciones proporcionados por XenApp y XenDesktop estén disponibles en la tienda, siga los pasos descritos en Cómo agregar recursos de XenDesktop y XenApp a la tienda. Después de agregar todos los recursos necesarios a la tienda, vuelva al paso 7 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

Limitación: Las aplicaciones publicadas en AppController pueden no iniciarse. Como solución temporal, use los comandos PowerShell de StoreFront para crear manualmente una tienda con un servicio de autenticación ubicado en **http://***sfserver***/Citrix/Authentication.**

Cómo proporcionar acceso remoto a la tienda a través de un dispositivo NetScaler Gateway

Complete los siguientes pasos para configurar el acceso remoto a través de un dispositivo NetScaler Gateway a la tienda que crea como parte de la configuración inicial del servidor StoreFront. Se presupone que usted ha completado los pasos 1 - 9 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

1. En la página Acceso remoto del asistente Crear tienda en la consola de StoreFront, haga clic en Agregar.
2. En el cuadro de diálogo Agregar dispositivo NetScaler Gateway, especifique un nombre para el dispositivo que ayude a los usuarios a identificarlo.
   Los usuarios verán el nombre simplificado que especifique en Citrix Receiver, de modo que debe incluir la información relevante en el nombre para ayudarles a decidir si desean utilizar ese dispositivo o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de NetScaler Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.

3. Escriba la URL del servidor virtual o punto de entrada del usuario (si utiliza Access Gateway 5.0) para el dispositivo. Especifique la versión de producto utilizada en la implementación.
   Para obtener información sobre cómo crear un único nombre de dominio completo para acceder a una tienda interna y externamente, consulte Creación de un nombre de dominio completo (FQDN) para acceder a una tienda de forma interna y externa.

4. Si desea agregar un dispositivo Access Gateway 5.0, seleccione Dispositivo de la lista Modo de implementación. De lo contrario, especifique la dirección IP de subred del dispositivo NetScaler Gateway, si es necesario. Se necesita una dirección IP de subred para los dispositivos Access Gateway 9.3. Esta dirección es optativa si se trata de versiones más

recientes de producto.
La dirección de subred es la dirección IP que NetScaler Gateway utiliza para representar el dispositivo de usuario cuando se comunica con los servidores de la red interna. También puede ser la dirección IP asignada del dispositivo NetScaler Gateway. Cuando está especificada, StoreFront utiliza la dirección IP de subred para verificar que las solicitudes entrantes provienen de un dispositivo de confianza.

5. Si desea agregar un dispositivo con NetScaler Gateway 10.1, Access Gateway 10 o Access Gateway 9.3, seleccione en la lista Tipo de inicio de sesión el método de autenticación configurado en el dispositivo para los usuarios de Citrix Receiver. La información que proporcione sobre la configuración de su dispositivo NetScaler Gateway se agrega al archivo de aprovisionamiento para la tienda. Esto permite que Citrix Receiver envíe la solicitud de conexión pertinente al comunicarse con el dispositivo por primera vez.

   - Si es necesario que los usuarios introduzcan sus credenciales de dominio de Microsoft Active Directory, seleccione Dominio.
   - Si es necesario que los usuarios introduzcan un código de token obtenido de un token de seguridad, seleccione Token de seguridad.
   - Si es necesario que los usuarios introduzcan sus credenciales de dominio y un código de token obtenido de un token de seguridad, seleccione Dominio y token de seguridad.
   - Si es necesario que los usuarios introduzcan una contraseña de un solo uso enviada por mensaje de texto, seleccione Autenticación SMS.
   - Si es necesario que los usuarios presenten una tarjeta inteligente e introduzcan un PIN, seleccione Tarjeta inteligente.

   Si configura la autenticación con tarjeta inteligente con un método secundario de autenticación (al que los usuarios puedan recurrir en caso de tener problemas con su tarjeta inteligente), seleccione el método secundario de autenticación en la lista Alternativa a tarjeta inteligente.

6. Complete la URL del servicio de autenticación de NetScaler Gateway en el cuadro URL de respuesta. StoreFront anexa automáticamente la parte estándar de la dirección URL. Haga clic en Siguiente.
   Escriba la URL internamente accesible del dispositivo. StoreFront se comunica con el servicio de autenticación de NetScaler Gateway para verificar que las solicitudes recibidas de NetScaler Gateway provienen de ese dispositivo.

7. Si desea que los recursos proporcionados por XenDesktop o XenApp estén disponibles en la tienda, enumere en la página Secure Ticket Authority (STA) las direcciones URL de los servidores que ejecutan el STA. Introduzca direcciones URL vinculadas a varios STA para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error.
   El STA está alojado en servidores XenDesktop y XenApp. Emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.

8. Si desea que XenDesktop y XenApp mantengan abiertas las sesiones desconectadas mientras Citrix Receiver intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y desea asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tiquets de dos STA, si están disponibles.
   Cuando la casilla Solicitar tiquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tiquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA no está disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.

9. Haga clic en Crear para agregar la implementación de NetScaler Gateway a la lista en la página Acceso remoto.

Para agregar más implementaciones, repita el procedimiento anterior. Para configurar el acceso remoto a la tienda a través de un clúster de Access Gateway 5.0, siga los pasos descritos en Cómo proporcionar acceso remoto a la tienda a través de un clúster de Access Gateway 5.0. Después de agregar todas las implementaciones de NetScaler Gateway, vuelva al paso 10 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

Cómo proporcionar acceso remoto a la tienda a través de un clúster de Access Gateway 5.0

Complete los siguientes pasos para configurar el acceso remoto a través de un clúster de Access Gateway 5.0 a la tienda que usted cree como parte de la configuración inicial del servidor StoreFront. Se presupone que usted ha completado los pasos 1 - 9 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

1. En la página Acceso remoto del asistente Crear tienda en la consola de StoreFront, haga clic en Agregar.
2. En el cuadro de diálogo Agregar dispositivo NetScaler Gateway, especifique un nombre para el clúster que ayude a los usuarios a identificarlo.
   Los usuarios verán el nombre simplificado que especifique en Citrix Receiver, de modo que debe incluir la información relevante en el nombre para ayudarlos a decidir si desean utilizar ese clúster o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de NetScaler Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.
3. Introduzca la URL del punto de entrada del usuario para el clúster y seleccione 5.x de la lista Versión.
4. Seleccione Access Controller de la lista Modo de implementación y haga clic en Siguiente.
5. En la página Dispositivos, enumere las direcciones IP o los FQDN de los dispositivos del clúster y haga clic en Siguiente.
6. En la página Habilitar autenticación silenciosa, enumere las direcciones URL para el servicio autenticación que se ejecuta en los servidores de Access Controller. Agregue direcciones URL de varios servidores para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Haga clic en Siguiente.
   StoreFront utiliza el servicio de autenticación para realizar la autenticación de los usuarios remotos para que no necesiten volver a introducir sus credenciales cuando accedan a las tiendas.
7. Si desea que los recursos proporcionados por XenDesktop y XenApp estén disponibles en la tienda, enumere en la página Secure Ticket Authority (STA) las direcciones URL de los servidores que ejecutan el STA. Introduzca direcciones URL vinculadas a varios STA para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error.
   El STA está alojado en servidores XenDesktop y XenApp. Emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.
8. Si desea que XenDesktop y XenApp mantengan abiertas las sesiones desconectadas mientras Citrix Receiver intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y desea asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tiquets de dos STA, si están disponibles.
   Cuando la casilla Solicitar tiquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tiquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA no está disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.
9. Haga clic en Crear para agregar la implementación de NetScaler Gateway a la lista en la página Acceso remoto.

Para agregar más clústeres, repita el procedimiento anterior. Para configurar el acceso remoto a la tienda a través de

NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3 o un dispositivo único Access Gateway 5.0, siga los pasos descritos en Cómo proporcionar acceso remoto a la tienda a través de un dispositivo NetScaler Gateway. Después de agregar todas las implementaciones de NetScaler Gateway, vuelva al paso 10 del procedimiento "Creación de una nueva implementación" en la parte superior de este artículo.

Incorporación a un grupo de servidores existente

Aug 14, 2017

Antes de instalar StoreFront, asegúrese de que el servidor que está agregando al grupo está ejecutando la misma versión de sistema operativo con la misma configuración regional que el resto de los servidores del grupo. No se respaldan los grupos de servidores StoreFront que contengan combinaciones de versiones de sistema operativo y configuraciones regionales. Aunque un grupo de servidores puede contener hasta cinco servidores como máximo, desde el punto de vista de la capacidad basada en simulaciones, no hay ventaja alguna en crear grupos que contengan más de tres servidores. Además, debe asegurarse de que la ruta relativa a StoreFront en IIS en el servidor que intenta agregar es el mismo que el resto de los servidores en el grupo.

> ## Important
>
> Cuando agrega un nuevo servidor a un grupo de servidores, las cuentas de servicio de StoreFront se agregan como miembros del grupo de administradores locales en el nuevo servidor. Estos servicios requieren permisos de administrador local para unirse y sincronizarse con el grupo de servidores. Si usa Directivas de grupo para impedir la incorporación de nuevos miembros al grupo de administradores locales, o si tiene restringidos los permisos del grupo de administradores locales en los servidores, StoreFront no puede incorporarse al grupo de servidores.

1. Si la consola de administración de Citrix StoreFront aún no está abierta después de la instalación de StoreFront, haga clic en la pantalla Inicio o Aplicaciones de Windows y haga clic en el icono Citrix StoreFront.
2. En el panel de resultados de la consola de administración de Citrix StoreFront, haga clic en Incorporarse a un grupo de servidores existente.
3. Inicie sesión en un servidor de la implementación de StoreFront a la que desea unirse y abra la consola de administración de Citrix StoreFront. Seleccione el nodo Grupo de servidores en el panel izquierdo de la consola y, en el panel Acciones, haga clic en Agregar servidor. Anote el código de autorización que aparece.
4. Vuelva al nuevo servidor y, en el cuadro de diálogo Incorporarse a grupo de servidores, especifique el nombre del servidor existente en el cuadro Servidor de autorización. Introduzca el código de autorización obtenido a partir de ese servidor y haga clic en Incorporarse.
   Una vez incorporado al grupo, la configuración del nuevo servidor se actualiza para que coincida con la configuración del servidor existente. Todos los demás servidores del grupo se actualizan con la información del nuevo servidor.

Para administrar implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Cualquier cambio de configuración realizado debe propagarse a los demás servidores para garantizar una configuración coherente en toda la implementación.

Quitar un servidor de un grupo de servidores existente

Si un servidor StoreFront era miembro de un grupo de servidores y fue eliminado, es necesario ejecutar el cmdlet de PowerShell Clear-DSConfiguration para restablecer el servidor StoreFront al estado predeterminado de fábrica. Después de ejecutar el cmdlet Clear-DSConfiguration en el servidor desconectado, puede agregar de nuevo el servidor a un grupo de servidores existente o a otro grupo de servidores nuevo que haya creado.

1. Abra la consola de administración de StoreFront en el servidor StoreFront principal que use para administrar el grupo de servidores entero.

2. Seleccione el nodo del grupo de servidores en el panel izquierdo y elija el servidor que quiere quitar.
3. Quite el servidor seleccionado del grupo de servidores.
4. En el panel Acciones, propague los cambios desde el servidor utilizado para desconectar uno de los miembros del grupo de servidores. Con esta acción, ahora los demás miembros del grupo registran que un servidor ha sido quitado del grupo. Hasta que el servidor desconectado sea restablecido al estado predeterminado de fábrica, dicho servidor no registrará que ya no es miembro del grupo.
5. Cierre la consola de administración en el servidor desconectado.
6. Abra una sesión de PowerShell en el servidor desconectado después de haberlo quitado del grupo e importe los módulos de PowerShell de StoreFront usando: & "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.ps1"
7. Ejecute el comando Clear-DSConfiguration, que restablece el servidor a sus parámetros predeterminados.
8. Abra la consola de administración de StoreFront y el servidor estará restablecido y listo para ser agregado a otro grupo de servidores.

Migración de funciones de la Interfaz Web a StoreFront

Aug 14, 2017

Muchas de las personalizaciones de la Interfaz Web tienen su equivalente en StoreFront y se pueden configurar usando ajustes de JavaScript, API publicadas de Citrix o la consola de administración de StoreFront.

La tabla ofrece información general acerca de las personalizaciones, así como información básica sobre cómo conseguirlas.

Ubicaciones de carpetas

- Para las personalizaciones de script, agregue los ejemplos al archivo script.js, ubicado en:

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

- Para las personalizaciones de estilo, agregue el ejemplo al archivo style.css, ubicado en:

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

- Para el contenido dinámico, agregue el contexto dinámico a un archivo de texto ubicado en:

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

- Si la suya es una implementación de varios servidores, puede replicar los cambios a los demás servidores desde la consola de administración de StoreFront o mediante PowerShell.

Nota: La Interfaz Web permite que usuarios individuales puedan personalizar varios parámetros. Actualmente, StoreFront no tiene esta capacidad y, aunque es posible agregar una personalización más amplia para admitirla, explicar ese procedimiento no es el objetivo de este artículo.

Función de la Interfaz Web	**Equivalente de StoreFront**
Personalización con la consola de administración	
• Distribución sin gráficos • Distribución con gráficos • Permitir que los usuarios elijan	No aplicable. StoreFront detecta y ajusta automáticamente la interfaz de usuario a la pantalla del dispositivo.
• Habilitar búsqueda • Inhabilitar búsqueda	• La búsqueda está habilitada de forma predeterminada. • Inhabilitar: Para ocultar los cuadros de búsqueda en la interfaz de usuario Web o del escritorio, agregue el siguiente estilo al archivo style.css: **.search-container {** **display: none;**

	} Para ocultar los cuadros de búsqueda en la interfaz de usuario del teléfono, agregue: **#searchBtnPhone {** **display: none;** **}**
Habilitar actualización	Habilitada de forma predeterminada (actualización del explorador).
Habilitar retorno a la última carpeta	No habilitada de forma predeterminada. Habilitar retorno a la última carpeta. Para recordar la carpeta actual y volver a ella al cargar, agregue lo siguiente a script.js: **CTXS.Extensions.afterDisplayHomeScreen = function ()** **{** **// comprobar si la vista se guardó la última vez** **CTXS.ExtensionAPI.localStorageGetItem("view",** **function (view) {** **if (view) {** **// si la vista se guardó, cambiar a ella** **CTXS.ExtensionAPI.changeView(view);** **}** **if (view == "store") {** **// si la vista es "store", ver si se guardó la carpeta** **CTXS.ExtensionAPI.localStorageGetItem("folder",** **function(folder) {** **if (folder != "") {** **// si la carpeta se guardó, cambiar a ella** **CTXS.ExtensionAPI.navigateToFolder(folder);** **}** **}**

	);
	}
	// configurar la supervisión de carpeta
	CTXS.Extensions.onFolderChange = function(folder) {
	CTXS.ExtensionAPI.localStorageSetItem("folder",
	folder);
	};
	// configurar la supervisión de vistas
	CTXS.Extensions.onViewChange = function(newview) {
	// no conservar las vistas de búsqueda o información de aplicación
	// en vez de ello, recordar la vista de nivel superior.
	if ((newview != "appinfo") &&
	(newview != "search")) {
	CTXS.ExtensionAPI.localStorageSetItem(
	"view", newview);
	}
	};
	});
	};

Habilitar sugerencias	Citrix Receiver utiliza muy poco los cuadros de información sobre herramientas, ya que está orientado tanto a los dispositivos táctiles como a los que no son táctiles. Puede agregar cuadros de información sobre herramientas mediante scripts personalizados.
• Vista de iconos • Vista de árbol • Vista de detalles • Vista de lista • Vista de grupo • Establecer vista predeterminada • Vista de iconos (sin gráficos) • Vista de lista (sin gráficos) Vista predeterminada (sin gráficos)	Citrix Receiver tiene una interfaz de usuario diferente, así que estas opciones no se aplican. Puede usar la consola de administración de StoreFront para configurar las vistas. Para obtener más información, consulte Cómo especificar diferentes vistas de aplicaciones y escritorios.

• Interfaz de usuario de ficha única
• Interfaz de usuario por fichas
  • Ficha Aplicaciones
  • Ficha Escritorio
  • Ficha Contenido
  • (Orden de las fichas)
	De forma predeterminada, la interfaz de usuario de Citrix Receiver está organizada en fichas, con aplicaciones y contenido en una ficha y escritorios en la otra. También existe la ficha optativa **Favoritos**.

• Logo de encabezado • Color de texto • Color de fondo del encabezado • Imagen de fondo del encabezado	Equivalentes para colores y logos mediante la consola de administración de StoreFront. En el panel "Acciones" de la consola de administración de StoreFront, haga clic en "Personalizar apariencia del sitio Web" y lleve a cabo sus personalizaciones en la pantalla que se muestra. Puede establecer una imagen de fondo para el encabezado con una personalización de estilo. Por ejemplo: **.theme-header-bgcolor {** **background-image: url('spirals.png');** **}**

• Mensaje de bienvenida previo al inicio de sesión
(Anterior a la configuración regional)
  • Título
  • Texto
  • Hipervínculo
  • Etiqueta de botón
	De forma predeterminada, no hay pantalla independiente en el preinicio de sesión.
	
	En este script de ejemplo se agrega un cuadro de mensaje por el que avanzar mediante clics:
	
	var doneClickThrough = false;
	
	// Antes del inicio de sesión Web
	
	CTXS.Extensions.beforeLogon = function (callback) {
	
	doneClickThrough = true;
	
	CTXS.ExtensionAPI.showMessage({
	
	messageTitle: "Welcome!",
	
	messageText: "Only for WWCo Employees",
	
	okButtonText: "Accept",
	
	okAction: callback
	
	});
	
	};
	
	// Antes de la pantalla principal (para clientes nativos)
	
	CTXS.Extensions.beforeDisplayHomeScreen

	= function (callback) { **if (!doneClickThrough) {** **CTXS.ExtensionAPI.showMessage({** **messageTitle: "Welcome!",** **messageText: "Only for WWCo Employees",** **okButtonText: "Accept",** **okAction: callback** **});** **} else {** **callback();** **}** **};**
• Título de la pantalla de inicio de sesión • Mensaje de la pantalla de inicio de sesión • Mensaje del sistema de la pantalla de inicio de sesión	Existen cuatro áreas de personalización en las pantallas de inicio de sesión. Parte superior e inferior de la pantalla (encabezado y pie de página) y parte superior e inferior del cuadro de inicio de sesión en sí. **.customAuthHeader,** **.customAuthFooter** **.customAuthTop,** **.customAuthBottom {** **text-align: center;** **color: white;** **font-size: 16px;** **}** Ejemplo de script (contenido estático) **$('.customAuthHeader').html("Welcome to ACME");** Ejemplo de script (contenido dinámico) **function setDynamicContent(txtFile, element) {** **CTXS.ExtensionAPI.proxyRequest({**

	url: "customweb/"+txtFile, **success: function(txt) {$(element).html(txt);}});** **}** **setDynamicContent("Message.txt", ".customAuthTop");** Nota: No incluya de forma explícita contenido dinámico en el script ni lo ponga en el directorio **custom**, ya que los cambios realizados aquí obligan a todos los clientes a volver a cargar la interfaz de usuario. Coloque el contenido dinámico en el directorio **customweb**.
• Mensaje de bienvenida de la pantalla de aplicaciones • Mensaje del sistema de la pantalla de aplicaciones	Consulte los ejemplos mencionados para la pantalla de bienvenida **CustomAuth**. Consulte los ejemplos anteriores para el contenido dinámico. Use **'#customTop'** en vez de **'.customAuthTop'** para colocar contenido en la pantalla principal.
Texto de pie de página (todas las pantallas)	Ejemplo de script: **#customBottom {** **text-align: center;** **color: white;** **font-size: 16px;** **}** Ejemplo de contenido estático con un script: **$('#customBottom').html("Welcome to ACME");**
Funciones sin equivalente directo	
• Pantalla de inicio de sesión sin encabezados • Pantalla de inicio de sesión con encabezados (incluidos los mensajes)	No existe equivalente directo en StoreFront. Sin embargo, puede crear encabezados personalizados. Consulte el apartado anterior llamado "Título de la pantalla de inicio de sesión".
Configuración de usuario	De forma predeterminada, no hay ninguna configuración de usuario. Puede agregar menús y botones desde JavaScript.

Control del espacio de trabajo	Funcionalidad equivalente para los parámetros del administrador. Las API de extensión permiten una flexibilidad adicional significativa. Consulte http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html.
Personalizaciones completas (código)	
Personalizaciones de conectores de llamadas y enlaces de generación de archivos ICA.	API equivalentes o mejores. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
Personalizaciones de autenticación	API equivalentes o mejores. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
Acceso al código JSP o ASP	No existe ninguna API equivalente en StoreFront, ya que la interfaz de usuario no se representa de la misma manera. Hay muchas API de JavaScript que permiten la personalización de la interfaz de usuario.

Configuración de grupos de servidores

Aug 14, 2017

Las tareas siguientes permiten modificar los parámetros de las implementaciones de StoreFront con varios servidores. Para administrar implementaciones con varios servidores, use solo un servidor a la vez para realizar cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Cualquier cambio de configuración realizado debe propagarse a los demás servidores para garantizar una configuración coherente en toda la implementación.

Los servidores incluidos en un grupo de servidores StoreFront deben estar todos configurados idénticamente, en términos de ubicación de la instalación de StoreFront y parámetros del sitio Web IIS, tales como la ruta física y el ID del sitio.

Incorporación de un servidor a un grupo de servidores

Utilice la tarea Agregar servidor para obtener un código de autorización que le permita unir un servidor StoreFront recién instalado a la implementación existente. Para obtener más información acerca de la incorporación de nuevos servidores a las implementaciones ya existentes de StoreFront, consulte Incorporación a un grupo de servidores existente.Consulte el apartado de *Escalabilidad* incluido en Planificación de una implementación de StoreFront para evaluar la cantidad necesaria de servidores en el grupo.

Eliminación de servidores de un grupo de servidores

Utilice la tarea Quitar servidor para quitar servidores de una implementación de StoreFront con varios servidores. Puede quitar cualquier servidor del grupo, excepto el servidor en el que ejecuta la tarea. Antes de quitar un servidor de una implementación con varios servidores, primero quite el servidor del entorno de equilibrio de carga.

Propagación de cambios locales en un grupo de servidores

Utilice la tarea Propagar cambios para actualizar la configuración de todos los demás servidores de una implementación de StoreFront con varios servidores de modo que coincida con la configuración del servidor actual. Se descarta cualquier cambio realizado en otros servidores del grupo. Mientras ejecuta esta tarea, no puede realizar cambios adicionales hasta que todos los servidores del grupo se hayan actualizado.

Importante: Si actualiza la configuración de un servidor sin propagar los cambios a los demás servidores del grupo, es posible que pierda las actualizaciones si posteriormente propaga los cambios desde otro servidor de la implementación.

Cambio de la dirección URL base para una implementación

Utilice la tarea Cambiar URL base para modificar la dirección URL que se usa como raíz para las direcciones URL de almacenes y otros servicios de StoreFront alojados en una implementación. Para las implementaciones con varios servidores, especifique la dirección URL con equilibrio de carga. Puede usar esta tarea para cambiar de HTTP a HTTPS siempre que quiera, con la condición de que Microsoft Internet Information Services (IIS) esté configurado para HTTPS.

Para configurar IIS para HTTPS, utilice la consola del administrador de Internet Information Services (IIS) en el servidor StoreFront, para crear un certificado de servidor firmado por la entidad de certificación del dominio de Microsoft Active Directory. A continuación, agregue un enlace HTTPS al sitio Web predeterminado. Para obtener más información acerca de la creación de un certificado de servidor en IIS, consulte http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate. Para obtener más información acerca de cómo agregar un enlace HTTPS a un sitio IIS, consulte http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding.

Configuración del comportamiento de omisión de servidores

Para mejorar el rendimiento cuando alguno de los servidores que proporcionan recursos deja de estar disponible, StoreFront omite temporalmente los servidores que no responden. Cuando un servidor se omite, StoreFront lo ignora y no lo utiliza para acceder a los recursos. Use estos parámetros para especificar la duración del comportamiento de omisión:

- **Duración de la omisión si no hay respuesta** especifica una duración reducida en minutos que StoreFront emplea en lugar de la duración indicada en **Omitir durante**, si se omiten todos los servidores de un Delivery Controller en particular. El valor predeterminado es 0 minutos.
- **Omitir durante** especifica el tiempo en minutos que StoreFront omite un servidor individual después de intentar ponerse en contacto sin éxito con dicho servidor. La duración de omisión predeterminada es 60 minutos.

Consideraciones al especificar el parámetro de Duración de la omisión si no hay respuesta

Al establecer un valor mayor en **Duración de la omisión si no hay respuesta**, se reduce el impacto causado por la falta de disponibilidad de un Delivery Controller concreto. Sin embargo, se produce un efecto negativo: los recursos de dicho Delivery Controller no estarán disponibles para los usuarios durante el tiempo especificado después de que se interrumpa temporalmente la red o de que el servidor no esté disponible. Considere la opción de usar valores más elevados para **Duración de la omisión si no hay respuesta** cuando se han configurado muchos Delivery Controllers para una tienda, especialmente Delivery Controllers que no son importantes y que no afectan al trabajo.

Al establecer un valor menor en **Duración de la omisión si no hay respuesta**, se aumenta la disponibilidad de los recursos ofrecidos por dicho Delivery Controller, pero también aumenta la posibilidad de generar esperas en el cliente si hay muchos Delivery Controllers configurados para una tienda y varios de ellos dejan de estar disponibles. Vale la pena mantener el valor predeterminado de 0 minutos cuando no se han configurado muchas comunidades y para Delivery Controllers importantes que afectan al trabajo.

Para cambiar los parámetros de omisión de una tienda

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Delivery Controllers**.
3. Seleccione un Controller, haga clic en **Modificar**, y luego haga clic en **Parámetros** en la pantalla **Modificar Delivery Controller**.
4. En la fila **Duración de la omisión si no hay respuesta**, haga clic en la segunda columna e introduzca el tiempo, en minutos, durante el cual un Delivery Controller se considera desconectado después de que ninguno de sus servidores haya respondido.
5. En la fila **Omitir durante**, haga clic en la segunda columna e introduzca el tiempo, en minutos, durante el cual se considera que un único servidor está desconectado si no ha respondido.

Configuración de la autenticación y la delegación

Aug 14, 2017

Según sus requisitos, hay varios métodos de autenticación y delegación.

Configuración del servicio de autenticación	El servicio de autenticación autentica a los usuarios para Microsoft Active Directory, garantizando que esos usuarios no necesiten iniciar sesión de nuevo para acceder a sus escritorios y aplicaciones.
Autenticación basada en el servicio XML	Si StoreFront no está en el mismo dominio que XenApp o XenDesktop, y no se pueden establecer relaciones de confianza de Active Directory, puede configurar StoreFront para que use el servicio XML de XenApp y XenDesktop para autenticar las credenciales de nombre de usuario y contraseña.
Delegación limitada de Kerberos para XenApp 6.5.	Utilice la tarea Configurar delegación Kerberos para especificar si StoreFront emplea una delegación Kerberos limitada en un único dominio para autenticarse en los Delivery Controllers.
Autenticación con tarjeta inteligente.	Configure la autenticación con tarjeta inteligente para todos los componentes de una implementación típica de StoreFront.
Período de notificación de caducidad de contraseña	Si permite que los usuarios de los sitios de Citrix Receiver para Web cambien sus contraseñas en cualquier momento, los usuarios locales cuyas contraseñas están a punto de caducar reciben una advertencia cuando inician sesión.

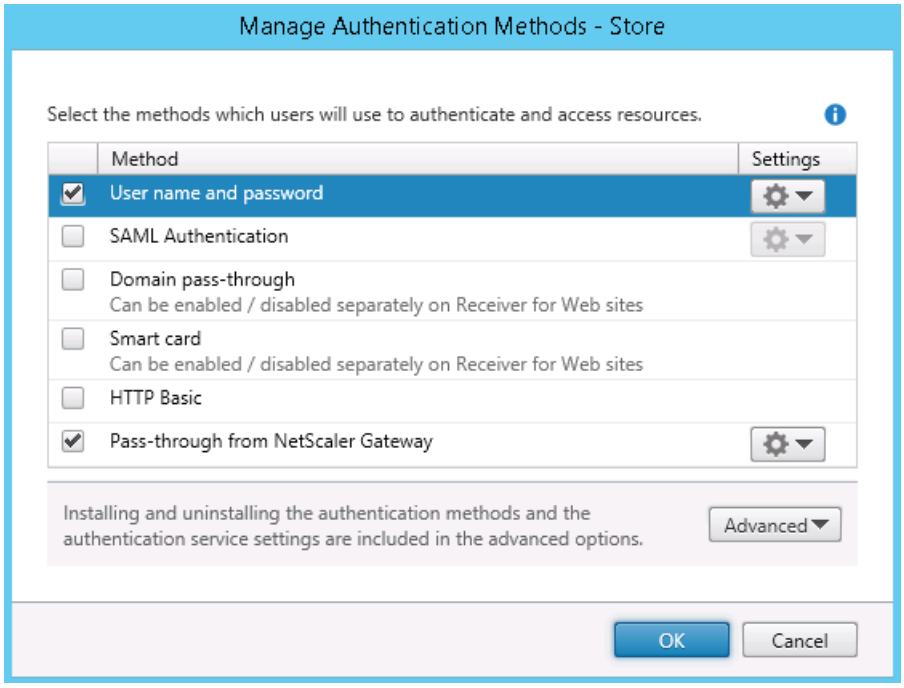
Configuración del servicio de autenticación

Aug 14, 2017

Administración de los métodos de autenticación

Para habilitar o inhabilitar la configuración de los métodos de autenticación de usuarios al crear el servicio de autenticación, seleccione un método de autenticación en el panel de resultados de la consola de administración de Citrix StoreFront y en el panel Acciones, haga clic en Administrar métodos de autenticación.

1. En la pantalla Inicio o Aplicaciones de Windows, busque el icono de Citrix **StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
3. Especifique los métodos de acceso que desea habilitar para los usuarios.



- Marque la casilla **Nombre de usuario y contraseña** para habilitar la autenticación explícita. Los usuarios introducen sus credenciales cuando acceden a sus tiendas.
- Marque la casilla **Autenticación SAML** para habilitar la integración con proveedores de identidades SAML. Los usuarios se autentican en un proveedor de identidades y su sesión se inicia automáticamente cuando acceden a sus tiendas.Desde el menú desplegable Parámetros:
  - Seleccione **Proveedor de identidades** para configurar la confianza con el proveedor de identidades.

- Seleccione **Proveedor de servicios** para configurar la confianza con el proveedor de servicios. El proveedor de identidades necesita esta información.

- Marque la casilla PassThrough de dominio para habilitar la autenticación PassThrough de las credenciales de dominio de Active Directory desde los dispositivos de los usuarios. Los usuarios realizan la autenticación en los equipos unidos a un dominio de Windows y su sesión se inicia automáticamente cuando acceden a las tiendas. Para poder usar esta opción, la autenticación PassThrough debe estar habilitada cuando se instala Citrix Receiver para Windows en los dispositivos de los usuarios.
- Marque la casilla Tarjeta inteligente para habilitar la autenticación con tarjeta inteligente. Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a las tiendas.
- Marque la casilla Básica HTTP para habilitar la autenticación básica HTTP. Los usuarios se autentican con el servidor Web IIS del servidor StoreFront.
- Marque la casilla PassThrough desde NetScaler Gateway para habilitar la autenticación PassThrough desde NetScaler Gateway. Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.

Para habilitar la autenticación PassThrough para los usuarios de tarjeta inteligente que acceden a las tiendas a través de NetScaler Gateway, use la tarea Configurar autenticación delegada.

Configuración de dominios de usuarios de confianza

Utilice la tarea Dominios de confianza para restringir el acceso a las tiendas de cara a los usuarios que inician sesión con credenciales de dominio explícitas, ya sea directamente o a través de la autenticación PassThrough desde NetScaler Gateway.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione el método de autenticación apropiado. En el panel Acciones, haga clic en **Administrar métodos de autenticación**.
3. En el menú desplegable **Nombre de usuario y contraseña (explícita) > Parámetros**, seleccione **Configurar dominios de confianza**.
4. Seleccione **Solo dominios de confianza** y haga clic en Agregar para introducir el nombre de un dominio de confianza. Los usuarios con cuentas en ese dominio podrán iniciar sesiones en todas las tiendas que usen el servicio de autenticación. Para modificar un nombre de dominio, seleccione la entrada correspondiente en Dominios de confianza y haga clic en Modificar. Seleccione un dominio de la lista y haga clic en Quitar para interrumpir el acceso a las tiendas para las cuentas de usuario en ese dominio.
   La manera en que se especifica el nombre del dominio determina el formato en el que los usuarios deben introducir sus credenciales. Si desea que los usuarios introduzcan sus credenciales en un formato de nombre de usuario de dominio, agregue el nombre NetBIOS a la lista. Para exigir que los usuarios introduzcan sus credenciales en el formato de nombre principal de usuario, agregue el FQDN a la lista. Si desea permitir que los usuarios introduzcan sus credenciales en el formato de nombre de usuario de dominio y en el formato de nombre principal de usuario, debe agregar el nombre NetBIOS y el FQDN a la lista.
5. Si configura varios dominios de confianza, seleccione de la lista Dominio predeterminado el dominio que aparece seleccionado de forma predeterminada cuando los usuarios inician sesión en StoreFront.
6. Si quiere ver una lista de los dominios de confianza en la página de inicio de sesión, marque la casilla Mostrar lista de dominios en la página de inicio de sesión.

Cómo permitir que los usuarios cambien sus contraseñas

Utilice la tarea **Administrar opciones de contraseña** para permitir que los usuarios de Receivers de escritorio y de sitios de Receiver para Web inicien sesión con credenciales de dominio para cambiar sus contraseñas. Al crear el servicio de autenticación, la configuración predeterminada impide que los usuarios de Citrix Receiver y de los sitios de Citrix Receiver para Web cambien sus contraseñas, incluso aunque hayan caducado. Si decide habilitar esta función, asegúrese de que las directivas para los dominios que contengan los servidores no impidan a los usuarios cambiar sus contraseñas. Cuando se

permite a los usuarios que cambien sus contraseñas, funciones importantes de seguridad se dejan a merced de cualquier persona que pueda acceder a las tiendas mediante el servicio de autenticación. Si su organización cuenta con una directiva de seguridad que solo permite utilizar las funciones de cambio de contraseñas de los usuarios para uso interno, asegúrese de que no se pueda acceder a las tiendas desde fuera de la red corporativa.

1. Citrix Receiver para Web admite cambios de contraseña por caducidad, así como cambios de contraseña a demanda. Los Citrix Receivers de escritorio admiten el cambio de contraseña a través de NetScaler Gateway solo por caducidad. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Administrar métodos de autenticación.
3. En el menú desplegable **Nombre de usuario y contraseña** > Parámetros, seleccione **Administrar opciones de contraseña** y especifique las circunstancias en las que los usuarios de los sitios de Citrix Receiver para Web que inician sesión con credenciales de dominio pueden cambiar sus contraseñas.
   - Para permitir que los usuarios cambien sus contraseñas cuando quieran, seleccione En cualquier momento. Cuando los usuarios locales cuyas contraseñas están a punto de caducar inicien sesión, aparecerá una advertencia al respecto. Las advertencias de caducidad de contraseña solo se muestran a los usuarios que se conectan desde la red interna. De forma predeterminada, el período de notificación para un usuario se determina mediante la configuración de directiva de Windows correspondiente. Para obtener más información sobre la configuración de períodos de notificación personalizados, consulte Configuración del período de notificación de caducidad de contraseñas. Solo respaldado con Citrix Receiver para Web.
   - Para permitir que los usuarios cambien sus contraseñas solamente cuando las contraseñas han caducado, seleccione Cuando caduquen. Los usuarios que no pueden iniciar sesión porque sus contraseñas han caducado se redirigen al cuadro de diálogo Cambiar contraseña. Respaldado en Citrix Receivers de escritorio y Citrix Receiver para Web.
   - Para impedir que los usuarios cambien sus contraseñas, no seleccione **Permitir a los usuarios cambiar sus contraseñas**. Si no selecciona esta opción, deberá organizar cómo dar respaldo a los usuarios que no puedan acceder a los escritorios y aplicaciones porque sus contraseñas hayan caducado.

   Si desea permitir que los usuarios de los sitios de Citrix Receiver para Web cambien sus contraseñas en cualquier momento, asegúrese de que haya suficiente espacio en disco en los servidores StoreFront para almacenar los perfiles de todos los usuarios. Para comprobar si la contraseña de un usuario está a punto de caducar, StoreFront crea un perfil local para ese usuario en el servidor. StoreFront debe poder ponerse en contacto con el controlador de dominio para cambiar las contraseñas de los usuarios.

Citrix Receivers	El usuario puede cambiar una contraseña caducada si está habilitada en StoreFront	Se notifica al usuario de que la contraseña va a caducar	El usuario puede cambiar la contraseña antes de que caduque si está habilitada en StoreFront
Windows	Sí		
Mac	Sí		
Android			
iOS			
Linux	Sí		

Citrix Web Receivers	El usuario puede cambiar una contraseña caducada si está habilitada en StoreFront	Se notifica al usuario de que la contraseña va a caducar	El usuario puede cambiar la contraseña antes de que caduque si está habilitada en StoreFront
	Sí	Sí	Sí

Preguntas de seguridad del Autoservicio de restablecimiento de contraseñas

El Autoservicio de restablecimiento de contraseñas o SSPR (Self-service Password Reset) permite que los usuarios finales tengan un mayor control sobre sus cuentas. Cuando el Autoservicio de restablecimiento de contraseñas está configurado, si los usuarios finales tienen problemas para iniciar sesión en sus sistemas, pueden desbloquear sus cuentas o restablecer sus contraseñas respondiendo correctamente a varias preguntas de seguridad.

Al configurar el Autoservicio de restablecimiento de contraseñas, usted especifica los usuarios que podrán restablecer contraseñas y desbloquear sus cuentas, usando la consola de administración. Aunque habilite esta funcionalidad para StoreFront, es posible que a los usuarios se les siga denegando el permiso para realizar estas tareas según cómo se hayan definido los parámetros en la consola de configuración del Autoservicio de restablecimiento de contraseñas.

El Autoservicio de restablecimiento de contraseñas solo está disponible para los usuarios que acceden a StoreFront mediante conexiones HTTPS. Si acceden a StoreFront mediante una conexión HTTP, el Autoservicio de restablecimiento de contraseñas no estará disponible para ellos. El Autoservicio de restablecimiento de contraseñas solo está disponible cuando la autenticación se realiza directamente con StoreFront usando un nombre de usuario y una contraseña.

El Autoservicio de restablecimiento de contraseñas no admite el uso de credenciales UPN para el inicio de sesión, tales como NombreDeUsuario@dominio.com.

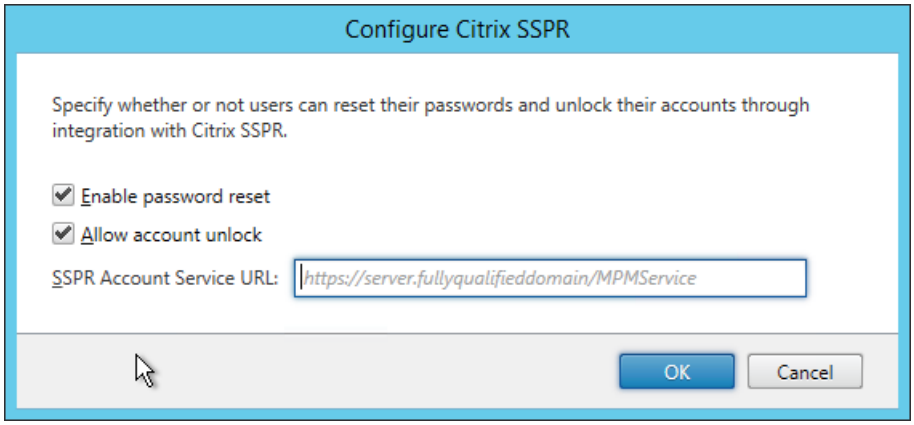
Antes de configurar el Autoservicio de restablecimiento de contraseñas para una tienda, debe asegurarse de lo siguiente:

- La tienda está configurada para usar autenticación con nombre de usuario y contraseña.
- La tienda está configurada para usar solo una instancia de Autoservicio de restablecimiento de contraseñas. Si StoreFront está configurado para utilizar varias comunidades en el mismo dominio o en dominios de confianza, el Autoservicio de restablecimiento de contraseñas debe configurarse para que acepte credenciales de todos esos dominios.
- El sitio debe configurarse para permitir que los usuarios cambien sus contraseñas en cualquier momento si se desea habilitar la funcionalidad de restablecimiento de contraseñas.
- Debe asociar una tienda de StoreFront a un sitio de Receiver para Web y debe configurar ese sitio para usar la experiencia unificada.

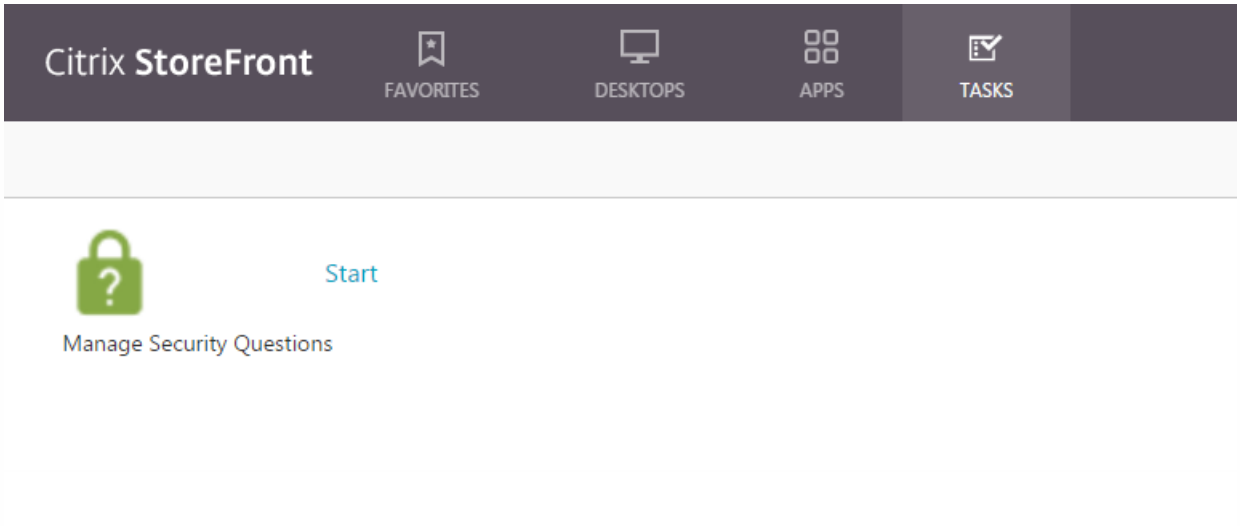
Antes de poder usar el Autoservicio de restablecimiento de contraseñas, hay que instalarlo y configurarlo. Está disponible en los medios de instalación de XenApp y XenDesktop.Para más información, consulte la documentación del Autoservicio de restablecimiento de contraseñas.

1. Para habilitar el respaldo para el Autoservicio de restablecimiento de contraseñas en StoreFront, seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación > Nombre de usuario y contraseña** y elija **Administrar opciones de contraseña** en el menú desplegable.
2. Elija cuándo quiere dejar que los usuarios cambien las contraseñas y haga clic en **Aceptar**.
3. En el menú desplegable **Nombre de usuario y contraseña**, elija **Configurar autoservicio de cuentas**, seleccione **Citrix SSPR en el menú desplegable**, y haga clic en **Aceptar.**
4. Especifique si se permite a los usuarios restablecer sus contraseñas y desbloquear sus cuentas con el Autoservicio de restablecimiento de contraseñas, agregue la dirección URL del servicio de restablecimiento de contraseñas, haga clic en **Aceptar** y de nuevo en **Aceptar.**

Esta opción solo está disponible cuando la URL base de StoreFront es HTTPS (no HTTP) y la opción **Habilitar el restablecimiento de contraseñas** solo está disponible después de usar **Administrar opciones de contraseña** para permitir a los usuarios cambiar sus contraseñas siempre que quieran.



La próxima vez que el usuario inicie sesión en Citrix Receiver o Citrix Receiver para Web, la inscripción de seguridad estará disponible. Después de hacer clic en **Iniciar**, el usuario verá preguntas a las que tiene que responder.

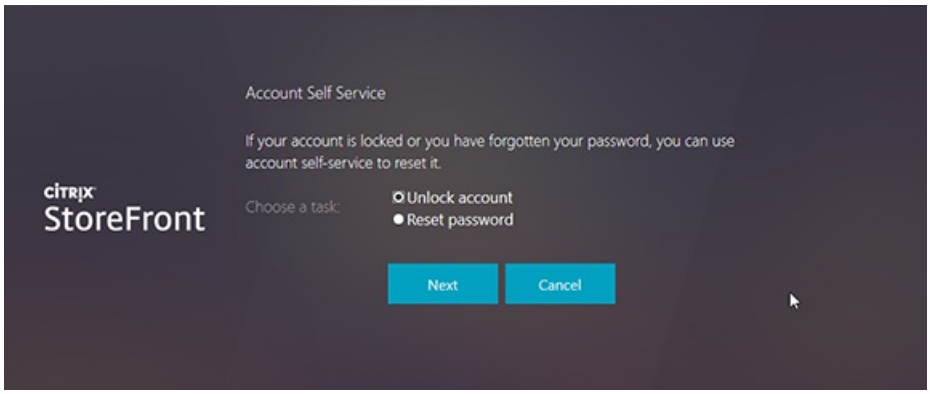


Una vez configurado en StoreFront, los usuarios verán el enlace de **Autoservicio de cuentas** en la pantalla de inicio de

sesión de Citrix Receiver para Web (se muestra como un botón en otras versiones de Citrix Receiver.

Al hacer clic en este enlace, el usuario ve una serie de formularios para seleccionar primero entre **Desbloquear cuenta** y **Restablecer contraseña** (si ambos están disponibles).

Después de elegir un botón de radio y hacer clic en **Siguiente**, la pantalla siguiente solicita el dominio y el nombre de usuario (*dominio**usuario*) si dicha información no se especificó antes en el formulario de inicio de sesión. Tenga en cuenta que el autoservicio de cuentas no admite el uso de credenciales UPN para el inicio de sesión, tales como NombreDeUsuario@dominio.com.



Los usuarios tienen que responder a las preguntas de seguridad. Si todas las respuestas coinciden con las respuestas que el usuario suministró, la operación solicitada (desbloqueo o restablecimiento) se lleva a cabo y el usuario recibe una notificación al respecto.

Parámetros del servicio de autenticación compartido

Utilice la tarea Parámetros del servicio de autenticación compartido para especificar las tiendas que compartirán el servicio de autenticación habilitando el inicio sesión Single Sign-on entre ellas.

1. En la pantalla **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
3. En el menú desplegable **Avanzado**, seleccione **Parámetros del servicio de autenticación compartido**.
4. Marque la casilla **Usar un servicio de autenticación compartido** y seleccione una tienda en el menú desplegable **Tienda**.

Nota: No hay ninguna diferencia funcional entre un servicio de autenticación compartido y uno dedicado. Un servicio de autenticación compartido entre dos o más tiendas se trata como uno solo y los cambios que se hagan en su configuración afectarán a todos las tiendas que lo comparten.

Delegar la validación de credenciales en NetScaler Gateway

Utilice la tarea Configurar autenticación delegada para habilitar la autenticación PassThrough para los usuarios de tarjeta inteligente que acceden a los almacenes a través de NetScaler Gateway. Esta tarea solo está disponible cuando la opción PassThrough desde NetScaler Gateway está habilitada y seleccionada en el panel de resultados.

Cuando la validación de credenciales se delega en NetScaler Gateway, los usuarios se autentican en NetScaler Gateway con sus tarjetas inteligentes e inician sesión automáticamente cuando acceden a las tiendas. De forma predeterminada, este parámetro está inhabilitado cuando habilita la autenticación PassThrough desde NetScaler Gateway. Por tanto, la autenticación PassThrough solo ocurre cuando los usuarios inician sesión en NetScaler Gateway con una contraseña.

Autenticación basada en el servicio XML

Aug 14, 2017

Si StoreFront no está en el mismo dominio que XenApp o XenDesktop, y no se pueden establecer relaciones de confianza de Active Directory, puede configurar StoreFront para que use el servicio XML de XenApp y XenDesktop para autenticar las credenciales de nombre de usuario y contraseña.

Habilitar la autenticación basada en el servicio XML

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar métodos de autenticación**.
3. En la página **Administrar métodos de autenticación**, en el menú **Nombre de usuario y contraseña > Parámetros**, seleccione **Configurar validación de contraseñas**.
4. En el menú desplegable **Validar contraseñas mediante**, seleccione **Delivery Controllers** y haga clic en **Configurar**.
5. Siga las instrucciones de las pantallas **Configurar Delivery Controllers** para agregar uno o varios **Delivery Controllers** para validar las credenciales de usuario y haga clic en **Aceptar**.

Inhabilitar la autenticación basada en el servicio XML

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar métodos de autenticación**.
3. En la página **Administrar métodos de autenticación**, en el menú **Nombre de usuario y contraseña** > **Parámetros**, seleccione **Configurar validación de contraseñas**.
4. En el menú desplegable **Validar contraseñas mediante**, seleccione **Active Directory** y haga clic en **Aceptar**.

Configuración de la delegación Kerberos limitada para XenApp 6.5

Aug 14, 2017

Utilice la tarea **Configurar parámetros de la tienda > Delegación de Kerberos** para especificar si StoreFront emplea una delegación de Kerberos limitada en un único dominio para autenticarse en los Delivery Controllers.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel Acciones, haga clic en **Configurar parámetros de la tienda** y, a continuación, haga clic en Delegación Kerberos.
3. Habilite o inhabilite la Delegación Kerberos para autenticarse en los Delivery Controllers.

Configuración del servidor StoreFront para la delegación

Siga este procedimiento cuando StoreFront no esté instalado en la misma máquina que XenApp.

1. En el controlador de dominio, abra el complemento Usuarios y equipos de Active Directory en la consola MMC.
2. En el menú Ver, haga clic en Características avanzadas.
3. En el panel izquierdo, haga clic en el nodo Equipos bajo el nombre de dominio y seleccione el servidor StoreFront.
4. En el panel Acción, haga clic en Propiedades.
5. En la ficha Delegación, haga clic en Confiar en este equipo para la delegación sólo a los servicios especificados y Usar cualquier protocolo de autenticación y, a continuación, haga clic en Agregar.
6. En el cuadro de diálogo Agregar servicios, haga clic en Usuarios o equipos.
7. En el cuadro de diálogo Seleccionar usuarios o equipos, escriba el nombre del servidor que ejecuta Citrix XML Service (XenApp) en el cuadro Escriba los nombres de objeto que quiere seleccionar y, a continuación, haga clic en Aceptar.
8. Seleccione el tipo de servicio HTTP en la lista y, a continuación, haga clic en Aceptar.
9. Aplique los cambios y cierre el cuadro de diálogo.

Configuración del servidor XenApp para la delegación

Configure la delegación de confianza de Active Directory para todos los servidores XenApp.

1. En el controlador de dominio, abra el complemento **Usuarios y equipos de Active Directory** en la consola MMC.
2. En el panel izquierdo, haga clic en el nodo **Equipos** debajo del nombre de dominio y seleccione el servidor que ejecuta Citrix XML Service (XenApp) con el que StoreFront está configurado para contactar.
3. En el panel **Acción**, haga clic en **Propiedades**.
4. En la ficha **Delegación**, haga clic en **Confiar en este equipo para la delegación sólo a los servicios especificados** y **Usar cualquier protocolo de autenticación** y, a continuación, haga clic en **Agregar**.
5. En el cuadro de diálogo **Agregar servicios**, haga clic en **Usuarios o equipos**.
6. En el cuadro de diálogo **Seleccionar usuarios o equipos**, escriba el nombre del servidor que ejecuta Citrix XML Service (XenApp) en el cuadro **Escriba los nombres de objeto que quiere seleccionar** y, a continuación, haga clic en **Aceptar**.
7. Seleccione el tipo de servicio HOST en la lista y, a continuación, haga clic en **Aceptar** y luego en **Agregar**.

8. En el cuadro de diálogo **Seleccionar usuarios o equipos**, escriba el nombre del controlador de dominio en el cuadro **Escriba los nombres de objeto que desea seleccionar** y, a continuación, haga clic en **Aceptar**.
9. Seleccione los tipos de servicio **cifs** y **ldap** de la lista y haga clic en **Aceptar**. Nota: Si aparecen dos opciones para el servicio ldap, seleccione la que coincida con el nombre de dominio completo (FQDN) del controlador de dominio.
10. Aplique los cambios y cierre el cuadro de diálogo.

Consideraciones importantes

Cuando deba decidir si quiere utilizar la delegación Kerberos limitada, tenga en cuenta la siguiente información.

- Notas importantes:
  - No necesita ssonsvr.exe a menos que realice la autenticación PassThrough (o la autenticación PassThrough con tarjeta inteligente con PIN) sin la delegación Kerberos limitada.
- Autenticación PassThrough de dominio para StoreFront y Citrix Receiver para Web:
  - No necesita ssonsvr.exe en el cliente.
  - Puede establecer el nombre de usuario y la contraseña locales que quiera en la plantilla icaclient.adm de Citrix (controla la función de ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - Agregue el nombre de dominio completo (FQDN) de StoreFront a la lista de sitios de confianza de Internet Explorer. Marque la casilla Usar nombre de usuario local en la configuración de seguridad de Internet Explorer para la zona de confianza.
  - El cliente debe estar en un dominio.
  - Habilite el método de autenticación PassThrough de dominio en el servidor StoreFront y habilítelo también para Citrix Receiver para Web.
- StoreFront, Citrix Receiver para Web y autenticación con tarjeta inteligente con solicitud de PIN:
  - No necesita ssonsvr.exe en el cliente.
  - La autenticación con tarjeta inteligente ya se ha configurado.
  - Puede establecer el nombre de usuario y la contraseña locales que quiera en la plantilla icaclient.adm de Citrix (controla la función de ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - Habilite el método de autenticación con tarjeta inteligente en el servidor StoreFront y habilítelo para Citrix Receiver para Web.
  - Para garantizar la elección de la autenticación con tarjeta inteligente, no marque la casilla Usar nombre de usuario local en la configuración de seguridad de Internet Explorer para la zona de sitios de StoreFront.
  - El cliente debe estar en un dominio.
- NetScaler Gateway, StoreFront, Citrix Receiver para Web y autenticación con tarjeta inteligente con solicitud de PIN:
  - No necesita ssonsvr.exe en el cliente.
  - La autenticación con tarjeta inteligente ya se ha configurado.
  - Puede establecer el nombre de usuario y la contraseña locales que quiera en la plantilla icaclient.adm de Citrix (controla la función de ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - Habilite el método de autenticación PassThrough desde NetScaler Gateway en el servidor StoreFront y habilítelo para Citrix Receiver para Web.
  - Para garantizar la elección de la autenticación con tarjeta inteligente, no marque la casilla Usar nombre de usuario local en la configuración de seguridad de Internet Explorer para la zona de sitios de StoreFront.
  - El cliente debe estar en un dominio.
  - Configure NetScaler Gateway para la autenticación con tarjeta inteligente y configure un servidor virtual adicional para que se inicie mediante el enrutamiento HDX de StoreFront para dirigir el tráfico ICA a través del servidor virtual no autenticado de NetScaler Gateway.
- Citrix Receiver para Windows (AuthManager), autenticación con tarjeta inteligente con petición de PIN y StoreFront:
  - No necesita ssonsvr.exe en el cliente.
  - Puede establecer el nombre de usuario y la contraseña locales que quiera en la plantilla icaclient.adm de Citrix (controla la función de ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - El cliente debe estar en un dominio.
  - Habilite el método de autenticación con Tarjeta inteligente en el servidor StoreFront.
- Citrix Receiver para Windows (AuthManager), Kerberos y StoreFront:
  - No necesita ssonsvr.exe en el cliente.
  - Puede establecer el nombre de usuario y la contraseña locales que quiera en la plantilla icaclient.adm de Citrix (controla la función de ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - Marque la casilla Usar nombre de usuario local en la configuración de seguridad de Internet Explorer para la zona de confianza.
  - El cliente debe estar en un dominio.
  - Habilite el método de autenticación PassThrough de dominio en el servidor StoreFront.
  - Compruebe que se ha definido esta clave de Registro:

    Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Debe

hacer una copia de seguridad del Registro antes de editarlo.

Para maquinas de 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwindows
Nombre: SSONCheckEnabled
Tipo: REG_SZ
Valor: true o false

Para máquinas de 64 bits:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocols\integratedwindows

Nombre: SSONCheckEnabled
Tipo: REG_SZ
Valor: true o false

Configuración de la autenticación con tarjeta inteligente

Aug 14, 2017

Este artículo ofrece una descripción general de las tareas de configuración de la autenticación con tarjeta inteligente para todos los componentes de una implementación típica de StoreFront. Para obtener más información y ver las instrucciones detalladas de la configuración, consulte la documentación de cada producto.

PDF

Configuración de tarjeta inteligente para entornos Citrix

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.

Requisitos previos

- Asegúrese de que las cuentas de todos los usuarios estén configuradas ya sea en el dominio Microsoft Active Directory en el que planea implementar los servidores StoreFront, o bien, dentro de un dominio que tenga una relación de confianza bidireccional directa con el dominio del servidor StoreFront.
- Si tiene pensado habilitar la autenticación PassThrough con tarjeta inteligente, asegúrese de que los tipos de lector de tarjeta inteligente, el tipo y la configuración de middleware y la directiva de almacenamiento en caché de PIN del middleware lo permiten.
- Instale el middleware de la tarjeta inteligente de su proveedor en las máquinas virtuales o físicas con el Virtual Delivery Agent que proporcionan los escritorios y las aplicaciones a los usuarios. Para obtener más información acerca del uso de tarjetas inteligentes con XenDesktop, consulte Tarjetas inteligentes.
- Antes de continuar, asegúrese de que la infraestructura de clave pública está configurada correctamente. Compruebe que la asignación de certificados a cuentas está configurada correctamente para el entorno de Active Directory y de que la validación de certificados de usuario puede realizarse correctamente.

Configuración de NetScaler Gateway

- En el dispositivo NetScaler Gateway, instale un certificado de servidor firmado por una entidad de certificación. Para obtener más información, consulte Instalación y administración de certificados.
- Instale en su dispositivo el certificado raíz de la entidad de certificación que emite los certificados de usuario de la tarjeta inteligente. Para obtener más información, consulte Para instalar un certificado raíz en NetScaler Gateway.
- Cree y configure un servidor virtual para la autenticación de certificados del cliente. Cree una directiva de autenticación de certificados y especifique SubjectAltName:PrincipalName para la extracción de nombres de usuario del certificado. A continuación, enlace la directiva con el servidor virtual y configure el servidor virtual para solicitar certificados del cliente. Para obtener más información, consulte Configuración y enlace de una directiva de autenticación de certificados del cliente.
- Enlace el certificado raíz de la entidad de certificación con el servidor virtual. Para obtener más información, consulte Para agregar un certificado raíz a un servidor virtual.
- Para asegurarse de que a los usuarios no se les vuelve a pedir las credenciales en el servidor virtual cuando se establecen conexiones con los recursos, cree un segundo servidor virtual. Cuando cree el servidor virtual, inhabilite la autenticación de cliente en los parámetros de Secure Sockets Layer (SSL). Para obtener más información, consulte Configuración de la autenticación con tarjeta inteligente.
  También debe configurar StoreFront para enrutar las conexiones de usuario a los recursos a través de este servidor virtual adicional. Los usuarios inician sesión en el primer servidor virtual y el segundo servidor virtual se utiliza para las conexiones

a los recursos. Cuando la conexión se establece, los usuarios no necesitan autenticarse en NetScaler Gateway pero tienen que introducir sus PIN para iniciar la sesión en sus escritorios y aplicaciones. La configuración de un segundo servidor virtual para las conexiones de usuario a los recursos es opcional, a menos que tenga pensado permitir que los usuarios recurran a la autenticación explícita si tienen problemas con las tarjetas inteligentes.

- Cree directivas y perfiles de sesión para conexiones de NetScaler Gateway a StoreFront y enlácelos al servidor virtual correspondiente. Para obtener más información, consulte Acceso a StoreFront a través de NetScaler Gateway.
- Si ha configurado el servidor virtual utilizado para las conexiones con StoreFront para exigir la autenticación de certificados del cliente para todas las comunicaciones, debe crear un servidor virtual adicional para proporcionar la URL de respuesta para StoreFront. Este servidor virtual solo se utiliza por StoreFront para comprobar las solicitudes del dispositivo NetScaler Gateway y, por lo tanto, no necesita ser públicamente accesible. Se requiere un servidor virtual independiente cuando la autenticación de certificados del cliente es obligatoria porque StoreFront no puede presentar un certificado para la autenticación. Para obtener más información, consulte Creating Virtual Servers.

Configuración de StoreFront

- Debe utilizar HTTPS para las comunicaciones entre los dispositivos de los usuarios y StoreFront para habilitar la autenticación con tarjeta inteligente. Configure Microsoft Internet Information Services (IIS) para HTTPS obteniendo un certificado SSL en IIS y agregando luego un enlace HTTPS al sitio Web predeterminado. Para obtener más información acerca de la creación de un certificado de servidor en IIS, consulte http://technet.microsoft.com/en-us/library/hh831637.aspx#CreateCertificate. Para obtener más información acerca de cómo agregar un enlace HTTPS a un sitio IIS, consulte http://technet.microsoft.com/en-us/library/hh831632.aspx#SSLBinding.
- Si desea exigir que se presenten certificados del cliente para las conexiones HTTPS con todas las direcciones URL de StoreFront, configure IIS en el servidor StoreFront.
  Cuando StoreFront se instala, la configuración predeterminada en IIS solo requiere que se presenten certificados del cliente para conexiones HTTPS con la URL de autenticación de certificados del servicio de autenticación de StoreFront. Esta configuración es necesaria para ofrecer a los usuarios de tarjetas inteligentes la opción de recurrir a la autenticación explícita y, según la configuración de directivas de Windows correspondiente, permitir que los usuarios puedan quitar las tarjetas inteligentes sin necesidad de volver a autenticarse.

  Cuando IIS está configurado para requerir certificados del cliente para conexiones HTTPS con todas las direcciones URL de StoreFront, los usuarios de tarjetas inteligentes no pueden conectarse a través de NetScaler Gateway y no pueden recurrir a la autenticación explícita. Los usuarios deben iniciar sesión de nuevo si quitan las tarjetas inteligentes de los dispositivos. Para habilitar esta configuración de sitio de IIS, el servicio de autenticación y las tiendas deben colocarse en el mismo servidor y debe utilizarse un certificado del cliente válido para todas las tiendas. Además, aquella configuración en la que IIS necesite certificados de cliente para conexiones HTTPS a todas las direcciones URL de StoreFront entrará en conflicto con la autenticación de los clientes Citrix Receiver para Web. Por esta razón, esta configuración debería utilizarse cuando no se necesite el acceso de clientes Citrix Receiver para Web.

  Si está instalando StoreFront en Windows Server 2012, tenga en cuenta que no se confía en los certificados no autofirmados instalados en el almacén de certificados Entidades de certificación raíz de confianza del servidor cuando IIS está configurado para utilizar SSL y la autenticación de certificado del cliente. Para obtener más información sobre este problema, consulte http://support.microsoft.com/kb/2802568.

- Instale y configure StoreFront. Cree el servicio de autenticación y agregue las tiendas según sea necesario. Si configura el acceso remoto a través de NetScaler Gateway, no habilite la integración de VPN. Para obtener más información, consulte Instalación y configuración de StoreFront.
- Habilite la autenticación con tarjeta inteligente en StoreFront para los usuarios locales de la red interna. Para los usuarios de tarjetas inteligentes que acceden a las tiendas a través de NetScaler Gateway, habilite el método de

autenticación PassThrough con NetScaler Gateway y asegúrese de que StoreFront está configurado para delegar la validación de credenciales en NetScaler Gateway. Si va a habilitar la autenticación PassThrough al instalar Citrix Receiver para Windows en dispositivos de usuario unidos a un dominio, habilite la autenticación PassThrough de dominio. Para obtener más información, consulte Configuración del servicio de autenticación.
Para permitir la autenticación de clientes Citrix Receiver para Web con tarjeta inteligente, debe habilitar dicho método de autenticación para cada sitio de Receiver para Web. Para obtener más información, consulte las instrucciones indicadas en Configuración de sitios de Citrix Receiver para Web.

Si desea que los usuarios de tarjetas inteligentes puedan recurrir a la autenticación explícita si tienen problemas con su tarjeta inteligente, no inhabilite el método de autenticación de nombre de usuario y contraseña.

- Si desea habilitar la autenticación PassThrough al instalar Citrix Receiver para Windows en los dispositivos de usuario unidos a un dominio, edite el archivo default.ica para la tienda en la que desea habilitar la autenticación PassThrough de credenciales con tarjeta inteligente de los usuarios cuando acceden a sus escritorios y aplicaciones. Para obtener más información, consulte Habilitación de la autenticación PassThrough con tarjeta inteligente en Citrix Receiver para Windows.
- Si ha creado un servidor virtual de NetScaler Gateway adicional para utilizarse únicamente en las conexiones de usuario a los recursos, configure el enrutamiento óptimo de NetScaler Gateway a través de este servidor virtual para las conexiones a las implementaciones que proporcionan los escritorios y las aplicaciones para la tienda. Para ver más información, consulte Configuración del enrutamiento óptimo de HDX para una tienda.
- Para permitir que los usuarios de dispositivos de escritorio de Windows no unidos a un dominio puedan iniciar sesión en sus escritorios con tarjetas inteligentes, habilite la autenticación con tarjeta inteligente en sus sitios de Desktop Appliance. Para obtener más información, consulte Configuración de los sitios de Desktop Appliance.

  Configure el sitio de Desktop Appliance para la autenticación con tarjeta inteligente y la autenticación explícita y, así, permitir a los usuarios iniciar sesión con credenciales explícitas si tienen problemas con las tarjetas inteligentes.

- Para permitir que los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados que ejecuten el Citrix Desktop Lock puedan autenticarse con tarjetas inteligentes, habilite la autenticación PassThrough con tarjeta inteligente para las direcciones URL de servicios XenApp. Para obtener más información, consulte Configuración de la autenticación de las direcciones URL de servicios XenApp.

Configuración de los dispositivos de usuario

- Asegúrese de que el middleware de las tarjetas inteligentes de su proveedor está instalado en los dispositivos de usuario.
- Para los usuarios con dispositivos de escritorio de Windows no unidos a un dominio, instale Receiver para Windows Enterprise mediante una cuenta con permisos de administrador. Configure Internet Explorer para iniciarse en modo de pantalla completa y mostrar el sitio de Desktop Appliance cuando el dispositivo se encienda. Tenga en cuenta que las direcciones URL de los sitios de Desktop Appliance distinguen entre mayúsculas y minúsculas. Agregue el sitio de Desktop Appliance en la zona de Intranet local o Sitios de confianza de Internet Explorer. Una vez que haya confirmado que puede iniciar sesión en el sitio de Desktop Appliance con una tarjeta inteligente y acceder a recursos de la tienda, instale el Citrix Desktop Lock. Para obtener más información, consulte Para instalar el Desktop Lock.
- Para los usuarios con dispositivos de escritorio no unidos a un dominio y equipos reasignados, instale Receiver para Windows (Enterprise) mediante una cuenta con permisos de administrador. Configure Receiver para Windows con la URL de servicios XenApp para la tienda correspondiente. Una vez que haya confirmado que puede iniciar sesión en el dispositivo con una tarjeta inteligente y acceder a recursos de la tienda, instale el Citrix Desktop Lock. Para obtener más información, consulte Para instalar el Desktop Lock.
- Para todos los demás usuarios, instale la versión de Citrix Receiver en el dispositivo de usuario. Para habilitar la

autenticación PassThrough de credenciales con tarjeta inteligente en XenDesktop y XenApp para los usuarios con dispositivos unidos a un dominio, use una cuenta con permisos de administrador para instalar Receiver para Windows en una ventana del símbolo del sistema con la opción /includeSSON. Para obtener más información, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.
Asegúrese de que Receiver para Windows está configurado para la autenticación con tarjeta inteligente a través de una directiva de dominio o una directiva de equipo local. Para una directiva de dominio, use la Consola de administración de directivas de grupo para importar el archivo de plantilla de objetos de directiva de grupo de Receiver para Windows, icaclient.adm, en el controlador de dominio para el dominio que contiene las cuentas de los usuarios. Para configurar un dispositivo individual, utilice el Editor de objetos de directiva de grupo en el dispositivo para configurar la plantilla. Para obtener más información, consulte Configuración de Receiver con la plantilla de objetos de directiva de grupo.

Habilite la directiva Autenticación con tarjeta inteligente. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente de los usuarios, seleccione Use pass-through authentication for PIN. A continuación, para la autenticación PassThrough de las credenciales con tarjeta inteligente de los usuarios a través de XenDesktop y XenApp, habilite la directiva Local user name and password y seleccione Allow pass-through authentication for all ICA connections. Para obtener más información, consulte Referencia para los parámetros ICA.

Si ha habilitado la autenticación PassThrough de credenciales con tarjeta inteligente en XenDesktop y XenApp para los usuarios con dispositivos unidos a un dominio, agregue la dirección URL de la tienda en la zona de Intranet local o Sitios de confianza de Internet Explorer. Asegúrese de que la opción Inicio de sesión automático con el nombre de usuario y contraseña actuales está seleccionada en la configuración de seguridad de la zona.

- Si es necesario, proporcione a los usuarios los datos de conexión para las tiendas (para los usuarios de la red interna) o los dispositivos NetScaler Gateway (para usuarios remotos) con un método adecuado. Para obtener más información sobre cómo proporcionar información de configuración a los usuarios, consulte Citrix Receiver.

Habilitación de la autenticación PassThrough con tarjeta inteligente en Receiver para Windows

Puede habilitar la autenticación PassThrough al instalar Receiver para Windows en los dispositivos de usuario unidos a un dominio. Para habilitar la autenticación PassThrough de credenciales de tarjeta inteligente de los usuarios cuando acceden a aplicaciones y escritorios alojados por XenDesktop y XenApp, modifique el archivo default.ica de la tienda.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Utilice un editor de texto para abrir el archivo default.ica de la tienda, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storename\App_Data\, donde storename es el nombre especificado para la tienda cuando se creó.
2. Para habilitar la autenticación PassThrough de credenciales de tarjeta inteligente para los usuarios que acceden a las tiendas sin NetScaler Gateway, agregue el siguiente parámetro en la sección [Application].
   DisableCtrlAltDel=Off
   Este parámetro se aplica a todos los usuarios de la tienda. Si desea habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear tiendas independientes para cada método de autenticación. A continuación, debe dirigir a los usuarios a la tienda adecuada para su método de autenticación.

3. Para habilitar la autenticación PassThrough de credenciales de tarjeta inteligente para los usuarios que acceden a las tiendas a través de NetScaler Gateway, agregue el siguiente parámetro en la sección [Application].

UseLocalUserAndPassword=On

Este parámetro se aplica a todos los usuarios de la tienda. Si desea habilitar la autenticación PassThrough para algunos usuarios y requerir que otros inicien sesión para acceder a sus escritorios y aplicaciones, debe crear tiendas independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios a la tienda adecuada para su método de autenticación.

Configuración del período de notificación de caducidad de contraseñas

Aug 14, 2017

Si permite que los usuarios de los sitios de Citrix Receiver para Web cambien sus contraseñas en cualquier momento, los usuarios locales cuyas contraseñas están a punto de caducar reciben una advertencia cuando inician sesión. De forma predeterminada, el período de notificación para un usuario se determina mediante la configuración de directiva de Windows correspondiente. Para establecer un período de notificación personalizada para todos los usuarios, edite el archivo de configuración para el servicio de autenticación.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar métodos de autenticación**.
3. En la página **Administrar métodos de autenticación**, en el menú desplegable **Nombre de usuario y contraseña** > **Parámetros**, seleccione **Administrar opciones de contraseña** y marque la casilla **Permitir a los usuarios cambiar sus contraseñas**.
4. Seleccione **En cualquier momento...** y elija una opción en la sección **Avisar a los usuarios antes de que caduquen sus contraseñas**.

Nota: StoreFront no admite directivas específicas de contraseña (fine-grained) en Active Directory.

Configuración y administración de tiendas

Aug 14, 2017

En Citrix StoreFront, puede crear y administrar tiendas que combinan escritorios y aplicaciones desde XenDesktop y XenApp, con lo que ofrecerá a los usuarios un acceso de autoservicio y a demanda a los recursos.

Crear o quitar una tienda	Configure tantas tiendas adicionales como necesite.
Creación de una tienda no autenticada	Configure más tiendas no autenticadas para permitir el acceso de usuarios no autenticados (anónimos).
Exportación de archivos de aprovisionamiento de tiendas para los usuarios	Genere archivos que contengan datos de conexión a las tiendas, incluidas las implementaciones de NetScaler Gateway y las balizas configuradas para las tiendas.
Formas de ocultar y publicar tiendas para los usuarios	Debe evitar que se muestren tiendas a los usuarios y, por tanto, que los puedan agregar a sus cuentas cuando configuren Citrix Receiver mediante la detección de cuentas basada en direcciones de correo electrónico o FQDN.
Administración de los recursos disponibles en tiendas	Agregue y quite recursos de las tiendas.
Administración del acceso remoto a las tiendas a través de NetScaler Gateway	Configure el acceso a las tiendas a través de NetScaler Gateway para los usuarios que se conectan desde redes públicas.
Integración de las aplicaciones de Citrix Online en las tiendas	Seleccione las aplicaciones de Citrix Online que quiere incluir en una tienda y especifique la acción que Citrix Receiver debe realizar cuando los usuarios se suscriban a una aplicación de Citrix Online.
Configuración de dos tiendas de StoreFront para compartir un almacén de datos de suscripción común	Configure dos tiendas para que compartan una base de datos de suscripción común.
Parámetros avanzados de las tiendas	Configure los parámetros avanzados de la tienda.

Crear o quitar una tienda

Aug 14, 2017

Utilice la tarea Crear tienda para configurar tiendas adicionales. Puede crear tantas tiendas como necesite. Por ejemplo: puede crear una tienda para un determinado grupo de usuarios o para agrupar un conjunto específico de recursos. También puede crear una tienda no autenticada que permita un uso anónimo o no autenticado. Para crear este tipo de tienda, consulte las instrucciones de la sección Creación de una tienda sin autenticación.

Para crear una tienda, identifique y configure las comunicaciones con los servidores que proporcionan los recursos que desea entregar mediante la tienda. A continuación, opcionalmente, configure el acceso remoto a la tienda a través de NetScaler Gateway.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Cómo agregar escritorios y aplicaciones a la tienda

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Crear tienda.
3. En la página Nombre de la tienda, especifique un nombre para la tienda y haga clic en Siguiente.
   Los nombres de las tiendas aparecen en Citrix Receiver en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido de la tienda.
4. En la página Delivery Controllers, enumere la infraestructura que proporciona los recursos que desea que estén disponibles en la tienda. Haga clic en Agregar.
5. En el cuadro de diálogo Agregar Delivery Controller, especifique un nombre que le ayude a identificar la implementación e indique si XenDesktop, XenApp o AppController proporcionan los recursos que desea poner a disposición a través de la tienda. En caso de implementaciones de App Controller, asegúrese de que el nombre especificado no contiene espacios.
6. Si quiere agregar información de los servidores XenDesktop o XenApp, continúe en el paso 7. Para que las aplicaciones que administra App Controller estén disponibles en la tienda, escriba el nombre o la dirección IP de un dispositivo virtual App Controller en el cuadro Servidor y especifique el puerto que StoreFront debe utilizar para las conexiones con App Controller. El puerto predeterminado es 443. Continúe en el paso 11.
7. Para ofrecer en la tienda los escritorios y las aplicaciones de XenDesktop y XenApp, agregue los nombres o las direcciones IP de los servidores a la lista Servidores. Especifique varios servidores para habilitar la tolerancia de fallos; para ello, enumere las entradas por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para los sitios de XenDesktop, proporcione información de los Delivery Controllers. En el caso de las comunidades de XenApp, enumere los servidores que ejecutan Citrix XML Service.
8. En la lista Tipo de transporte, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione HTTP. Si selecciona esta opción, deberá definir su propia configuración para proteger las conexiones entre StoreFront y los servidores.
   - Para enviar datos a través de conexiones HTTP seguras mediante SSL (Secure Sockets Layer) o TLS (Transport Layer Security), seleccione HTTPS. Si selecciona esta opción para servidores de XenDesktop y XenApp, asegúrese de que Citrix XML Service esté configurado para compartir su puerto con Microsoft Internet Information Services (IIS) y que IIS esté configurado para admitir HTTPS.

- Para enviar datos a través de conexiones seguras a servidores XenApp y utilizar el Traspaso SSL para realizar la autenticación del host y el cifrado de datos, seleccione Traspaso SSL.

Nota: Si utiliza HTTPS o el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres de servidores que especificó en la lista Servidores coincidan exactamente (incluidas mayúsculas y minúsculas) con los nombres en los certificados para esos servidores.

9. Especifique el puerto que StoreFront debe utilizar para las conexiones con los servidores. El puerto predeterminado para las conexiones que utilizan HTTP y el Traspaso SSL es 80, y para las conexiones mediante HTTPS es 443. En el caso de los servidores de XenDesktop y XenApp, el puerto especificado debe ser el puerto usado por Citrix XML Service.
10. Si utiliza el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores de XenApp, especifique el puerto TCP del Traspaso SSL en el cuadro Puerto del Traspaso SSL. El puerto predeterminado es 443. Asegúrese de que todos los servidores que ejecutan el Traspaso SSL estén configurados para escuchar en el mismo puerto.
11. Haga clic en Aceptar. Puede configurar las tiendas para que proporcionen recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y App Controller. Repita todos los pasos del 4 al 11, según sea necesario, para enumerar implementaciones adicionales que proporcionen recursos para la tienda. Una vez que haya agregado todos los recursos necesarios para la tienda, haga clic en Siguiente.
12. En la página Acceso remoto, especifique si los usuarios que se conectan desde redes públicas pueden acceder a la tienda a través de NetScaler Gateway y la forma en que pueden hacerlo.
    - Para hacer que la tienda no esté disponible para los usuarios de redes públicas, asegúrese de dejar sin marcar la casilla **Habilitar acceso remoto**. Solo los usuarios locales de la red interna podrán acceder a la tienda.
    - Para habilitar el acceso remoto, marque la casilla **Habilitar acceso remoto**.
        - Para que estén disponibles solo los recursos entregados por la tienda en NetScaler Gateway, seleccione Sin túnel VPN. Los usuarios inician sesión directamente en NetScaler Gateway y no necesitan usar el NetScaler Gateway Plug-in.
        - Para determinar que la tienda y todos los demás recursos de la red interna estén disponibles a través de un túnel VPN SSL, seleccione Túnel VPN completo. Los usuarios necesitan el NetScaler Gateway Plug-in para establecer el túnel VPN.

    Si no está habilitado, el método de autenticación PassThrough desde NetScaler Gateway se habilita automáticamente cuando se configura el acceso remoto a la tienda. Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.

13. Si ha habilitado el acceso remoto, continúe en el siguiente procedimiento para especificar las implementaciones de NetScaler Gateway a través de las cuales los usuarios pueden acceder a la tienda. De lo contrario, en la página Acceso remoto, haga clic en Crear. Después de haber creado la tienda, haga clic en Finalizar.

Cómo proporcionar acceso remoto a la tienda a través de NetScaler Gateway

Complete los siguientes pasos para configurar el acceso remoto a través de NetScaler Gateway a la tienda que ha creado en el procedimiento anterior. Se presupone que ha completado todos los pasos anteriores.

1. En la página **Acceso remoto** del asistente **Crear tienda**, seleccione, en la lista de **dispositivos NetScaler Gateway**, las implementaciones a través de las cuales los usuarios pueden acceder a la tienda. Las implementaciones configuradas anteriormente para otras tiendas pueden seleccionarse en la lista. Si desea agregar otra implementación a la lista, haga clic en Agregar. De lo contrario, continúe en el paso 12.
2. En el cuadro de diálogo **Agregar dispositivo NetScaler Gateway > Parámetros generales**, especifique un nombre para la implementación de NetScaler Gateway que ayude a los usuarios a identificarla.
   Los usuarios verán el nombre simplificado que especifique en Citrix Receiver, de modo que debe incluir la información relevante en el nombre para ayudarles a identificarlo y decidir si desean utilizar esa implementación o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de NetScaler Gateway, de

modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.

3. Escriba la URL del servidor virtual o punto de entrada de usuarios para la implementación. Especifique la versión de producto utilizada en la implementación.
   El nombre de dominio completo (FQDN) para la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de NetScaler Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de NetScaler Gateway.

4. Seleccione el uso de NetScaler Gateway entre las opciones disponibles.
   + **Autenticación y enrutamiento de HDX**: NetScaler Gateway se usará para la autenticación, así como para el enrutamiento de las sesiones HDX.
   + **Solo autenticación:** NetScaler Gateway se usará para la autenticación y no para el enrutamiento de sesiones HDX.
   + **Solo enrutamiento de HDX:** NetScaler Gateway se usará para enrutar sesiones HDX y no para la autenticación.
5. En la página Secure Ticket Authority (STA), si desea que los recursos proporcionados por XenDesktop o XenApp estén disponibles en la tienda, enumere en la página Secure Ticket Authority todas las direcciones URL de los servidores que ejecutan Secure Ticket Authority (STA). Introduzca direcciones URL vinculadas a varios STA para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error.

   El STA está alojado en servidores XenDesktop y XenApp. Emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.
6. Elija equilibrio de carga para Secure Ticket Authority. También puede especificar el intervalo de tiempo tras el cual se omitirá un STA que no responda.
7. Si desea que XenDesktop y XenApp mantengan abiertas las sesiones desconectadas mientras Citrix Receiver intenta volver a conectarse automáticamente, marque la casilla **Habilitar fiabilidad de la sesión**. Si configuró varios STA y desea asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla **Solicitar tiquets de dos STA, si están disponibles**. StoreFront obtiene tiquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA deja de estar disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.
8. En la página Parámetros de autenticación, seleccione la versión de NetScaler Gateway que quiere configurar.
9. Especifique la dirección IP de VServer del dispositivo NetScaler Gateway, si es necesario. Se necesita una dirección IP de VServer para los dispositivos Access Gateway 9.x. Esta dirección es optativa si se trata de versiones más recientes de producto. La dirección IP de VServer es la dirección IP que NetScaler Gateway utiliza para representar el dispositivo de usuario cuando se comunica con los servidores de la red interna. También puede ser la dirección IP asignada del dispositivo NetScaler Gateway. Cuando está especificada, StoreFront utiliza la dirección IP de VServer para verificar que las solicitudes entrantes provienen de un dispositivo de confianza.
10. En la lista Tipo de inicio de sesión, seleccione el método de autenticación configurado en el dispositivo para los usuarios de Citrix Receiver. La información que proporcione sobre la configuración de su dispositivo NetScaler Gateway se agrega al archivo de aprovisionamiento para la tienda. Esto permite que Citrix Receiver envíe la solicitud de conexión pertinente al comunicarse con el dispositivo por primera vez.

    - Si es necesario que los usuarios introduzcan sus credenciales de dominio de Microsoft Active Directory, seleccione Dominio.
    - Si es necesario que los usuarios introduzcan un código de token obtenido de un token de seguridad, seleccione Token de seguridad.
    - Si es necesario que los usuarios introduzcan sus credenciales de dominio y un código de token obtenido de un token

de seguridad, seleccione Dominio y token de seguridad.
- Si es necesario que los usuarios introduzcan una contraseña de un solo uso enviada por mensaje de texto, seleccione Autenticación SMS.
- Si es necesario que los usuarios presenten una tarjeta inteligente e introduzcan un PIN, seleccione Tarjeta inteligente.

Si configura la autenticación con tarjeta inteligente con un método secundario de autenticación (al que los usuarios puedan recurrir en caso de tener problemas con su tarjeta inteligente), seleccione el método secundario de autenticación en la lista Alternativa a tarjeta inteligente.

11. Introduzca la URL del servicio de autenticación de NetScaler Gateway en el cuadro URL de respuesta. Este campo es opcional. StoreFront anexa automáticamente la parte estándar de la dirección URL. Escriba la URL internamente accesible del dispositivo. StoreFront se comunica con el servicio de autenticación de NetScaler Gateway para verificar que las solicitudes recibidas de NetScaler Gateway provienen de ese dispositivo.
12. Haga clic en Crear para agregar la implementación de NetScaler Gateway a la lista en la página Acceso remoto. Repita todos los pasos del 1 al 11, según sea necesario, para agregar más implementaciones de NetScaler Gateway a la lista de dispositivos NetScaler Gateway. Si habilita el acceso a través de varias implementaciones mediante la selección de más de una entrada de la lista, especifique la implementación predeterminada que se utilizará para acceder a la tienda.
13. En la página Acceso remoto, haga clic en Crear. Después de haber creado la tienda, haga clic en Finalizar.

La tienda está ahora disponible para que los usuarios accedan a él mediante Citrix Receiver, el cual debe estar configurado con los datos de acceso a la tienda. Existen diversas maneras de proporcionar esta información a los usuarios y facilitares el proceso de configuración. Para obtener más información, consulte Opciones de acceso de usuarios.

De manera alternativa, los usuarios pueden acceder a la tienda a través del sitio de Receiver para Web, que permite que los usuarios accedan a sus escritorios y aplicaciones a través de una página Web. La URL de acceso a un sitio de Receiver para Web, utilizada para acceder a la nueva tienda, aparece al crearla.

Al crear una nueva tienda, la URL de servicios XenApp correspondiente se habilita de forma predeterminada. Los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados que ejecuten el Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a las tiendas directamente mediante la URL de servicios XenApp para la tienda. La dirección URL de servicios XenApp tiene el formato http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, donde serveraddress es el nombre de dominio completo (FQDN) del servidor o el entorno de equilibrio de carga para la implementación de StoreFront y storename es el nombre especificado para la tienda en el paso 3.

Creación de una tienda para implementaciones de un solo servidor en un servidor que no está unido a un dominio

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Crear tienda**.
3. En la página **Nombre de la tienda**, especifique un nombre para la tienda y haga clic en **Siguiente**.
   Los nombres de las tiendas aparecen en Citrix Receiver en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido de la tienda.

4. En la página **Delivery Controllers**, enumere la infraestructura que proporciona los recursos que desea que estén disponibles en la tienda. Haga clic en **Agregar**.
5. En el cuadro de diálogo **Agregar Delivery Controller**, especifique un nombre que lo ayude a identificar la implementación e indique si XenApp, XenDesktop o XenMobile AppController suministran los recursos que quiere poner en la tienda. En caso de implementaciones de App Controller, asegúrese de que el nombre especificado no contiene

espacios.

6. Si quiere agregar información de los servidores XenDesktop o XenApp, continúe en el paso 7. Para que las aplicaciones que administra App Controller estén disponibles en la tienda, escriba el nombre o la dirección IP de un dispositivo virtual App Controller en el cuadro Servidor y especifique el puerto que StoreFront debe utilizar para las conexiones con App Controller. El puerto predeterminado es 443. Continúe en el paso 11.
7. Para ofrecer en la tienda los escritorios y las aplicaciones de XenDesktop y XenApp, agregue los nombres o las direcciones IP de los servidores a la lista **Servidores**. Para los sitios de XenDesktop, proporcione información de los Delivery Controllers. En el caso de las comunidades de XenApp, enumere el servidor que ejecuta Citrix XML Service.
8. En la lista **Tipo de transporte**, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione HTTP. Si selecciona esta opción, deberá definir su propia configuración para proteger las conexiones entre StoreFront y el servidor.
   - Para enviar datos a través de conexiones HTTP seguras mediante SSL (Secure Sockets Layer) o TLS (Transport Layer Security), seleccione HTTPS. Si selecciona esta opción para servidores de XenDesktop y XenApp, asegúrese de que Citrix XML Service esté configurado para compartir su puerto con Microsoft Internet Information Services (IIS) y que IIS esté configurado para admitir HTTPS.
   - Para enviar datos a través de conexiones seguras a servidores XenApp y utilizar el Traspaso SSL para realizar la autenticación del host y el cifrado de datos, seleccione Traspaso SSL.

     Nota: Si utiliza HTTPS o el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres de servidores que especificó en la lista **Servidores** coincidan exactamente (incluidas mayúsculas y minúsculas) con el nombre que figura en el certificado del servidor.

9. Especifique el puerto que StoreFront debe utilizar para las conexiones con el servidor. El puerto predeterminado para las conexiones que utilizan HTTP y el Traspaso SSL es 80, y para las conexiones mediante HTTPS es 443. En el caso de los servidores de XenDesktop y XenApp, el puerto especificado debe ser el puerto usado por Citrix XML Service.
10. Si utiliza el Traspaso SSL para proteger las conexiones entre StoreFront y el servidor XenApp, especifique el puerto TCP del Traspaso SSL en el cuadro Puerto del Traspaso SSL. El puerto predeterminado es 443. Asegúrese de que todos los servidores que ejecutan el Traspaso SSL estén configurados para escuchar en el mismo puerto.
11. Hata clic en **Aceptar**. Puede configurar las tiendas para que proporcionen recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y App Controller. Repita todos los pasos del 4 al 11, según sea necesario, para enumerar implementaciones adicionales que proporcionen recursos para la tienda. Una vez que haya agregado todos los recursos necesarios para la tienda, haga clic en Siguiente.
12. En la página **Acceso remoto**, especifique si los usuarios que se conectan desde redes públicas pueden acceder a la tienda a través de NetScaler Gateway y la forma en que pueden hacerlo.
    - Si no desea que la tienda esté disponible para los usuarios de redes públicas, seleccione **Ninguno**. Solo los usuarios locales de la red interna podrán acceder a la tienda.
    - Para que estén disponibles solo los recursos entregados mediante NetScaler Gateway, seleccione **Sin túnel VPN**. Los usuarios inician sesión directamente en NetScaler Gateway y no necesitan usar el NetScaler Gateway Plug-in.
    - Para determinar que la tienda y todos los demás recursos de la red interna estén disponibles a través de un túnel VPN SSL, seleccione **Túnel VPN completo**. Los usuarios necesitan el NetScaler Gateway Plug-in para establecer el túnel VPN.

      Si no está habilitado, el método de autenticación PassThrough desde NetScaler Gateway se habilita automáticamente cuando se configura el acceso remoto a la tienda. Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.

13. Si ha habilitado el acceso remoto, continúe en el siguiente procedimiento Cómo proporcionar acceso remoto a la tienda a través de NetScaler Gateway para especificar las implementaciones de NetScaler Gateway a través de las cuales los usuarios pueden acceder a la tienda. De lo contrario, en la página **Acceso remoto**, haga clic en **Siguiente**.
14. En la página **Configurar métodos de autenticación**, seleccione el método por el cual los usuarios podrán autenticarse y acceder a los recursos, y haga clic en **Siguiente**.
15. En la página **Configurar validación de contraseñas**, seleccione los Delivery Controllers que ofrecen la validación de contraseñas y haga clic en **Siguiente**.
16. En la página **URL de servicios XenApp**, configure la dirección URL para los usuarios que no usan PNAgent para acceder a aplicaciones y escritorios y haga clic en **Crear**.

El **nodo de grupo de servidores** en el panel izquierdo y en el panel **Acciones** se reemplaza por **Cambiar URL base**. La única opción disponible es cambiar la URL base, porque los grupos de servidores no están disponibles en servidores que no están unidos a un dominio.

Quitar una tienda

Utilice la tarea Quitar tienda para eliminar una tienda. Al eliminar una tienda, también se eliminan los sitios asociados de Receiver para Web, los sitios de Desktop Appliance y las direcciones URL de servicios XenApp.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Creación de una tienda no autenticada

Aug 14, 2017

Utilice la tarea Crear tienda si quiere configurar más tiendas no autenticadas para respaldar el acceso de usuarios no autenticados (anónimos). Puede crear tantas tiendas no autenticadas como necesite. Por ejemplo: puede crear una tienda no autenticada para un determinado grupo de usuarios o para agrupar un conjunto específico de recursos.

El acceso remoto mediante NetScaler Gateway no se puede aplicar a tiendas no autenticadas.

Para crear una tienda no autenticada, identifique y configure las comunicaciones con los servidores que proporcionan los recursos que quiere poner en la tienda.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Cómo agregar escritorios y aplicaciones a la tienda

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Crear tienda.
3. En la página Nombre de la tienda, especifique un nombre para la tienda, seleccione **Permitir el acceso a esta tienda solo a usuarios no autenticados (anónimos)**, y haga clic en Siguiente.
   Los nombres de las tiendas aparecen en Citrix Receiver en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido de la tienda.
4. En la página **Delivery Controllers** enumere la infraestructura que proporciona los recursos que desea que estén disponibles en la tienda. Haga clic en Add.
5. En el cuadro de diálogo Agregar Delivery Controller, especifique un nombre que lo ayude a identificar la implementación e indique si XenApp o XenMobile (AppController) suministran los recursos que quiere poner la tienda. En caso de implementaciones de XenMobile (AppController), asegúrese de que el nombre especificado no contenga espacios. Al asignar Controllers, compruebe que está utilizando únicamente aquellos que admitan la función de aplicaciones anónimas. Si configura su tienda no autenticada con Controllers que no admiten esta función, es posible que no haya ninguna aplicación anónima disponible en la tienda.
6. Si quiere agregar información detallada sobre los servidores XenApp, continúe en el paso 7. Para que las aplicaciones que administra XenMobile (AppController) estén disponibles en la tienda, escriba el nombre o la dirección IP de un dispositivo virtual XenMobile (AppController) en el cuadro Servidor y especifique el puerto que debe utilizar StoreFront para las conexiones con XenMobile (AppController). El puerto predeterminado es 443. Continúe en el paso 10.
7. Para que los escritorios y las aplicaciones que ofrece XenApp estén disponibles en la tienda, agregue los nombres o las direcciones IP de sus servidores a la lista Servidores. Especifique varios servidores para habilitar la tolerancia de fallos; para ello, enumere las entradas por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para los sitios de XenDesktop, proporcione información de los Controllers. En el caso de las comunidades de XenApp, enumere los servidores que ejecutan Citrix XML Service.
8. En la lista Tipo de transporte, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione HTTP. Si selecciona esta opción, deberá definir su propia configuración para proteger las conexiones entre StoreFront y los servidores.
   - Para enviar datos a través de conexiones HTTP seguras mediante SSL (Secure Sockets Layer) o TLS (Transport Layer

Security), seleccione HTTPS. Si selecciona esta opción para servidores de XenDesktop y XenApp, asegúrese de que Citrix XML Service esté configurado para compartir su puerto con Microsoft Internet Information Services (IIS) y que IIS esté configurado para admitir HTTPS.

Nota: Si utiliza HTTPS para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres especificados en la lista Servidores coincidan exactamente (incluidas mayúsculas y minúsculas) con los nombres que constan en los certificados para dichos servidores.

9. Especifique el puerto que StoreFront debe utilizar para las conexiones con los servidores. El puerto predeterminado para las conexiones que utilizan HTTP es 80, y para las conexiones mediante HTTPS es 443. En el caso de los servidores de XenDesktop y XenApp, el puerto especificado debe ser el puerto usado por Citrix XML Service.
10. Haga clic en Aceptar. Puede configurar las tiendas para que proporcionen recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y App Controller. Repita todos los pasos del 4 al 10, según sea necesario, para enumerar implementaciones adicionales que proporcionen recursos para la tienda. Una vez que haya agregado todos los recursos necesarios a la tienda, haga clic en Crear.

Ahora ya podrá utilizar la tienda no autenticada. Para habilitar el acceso de usuarios a la nueva tienda, Citrix Receiver debe configurarse con la información de acceso de la tienda. Existen diversas maneras de proporcionar esta información a los usuarios y facilitares el proceso de configuración. Para obtener más información, consulte Opciones de acceso de usuarios. De manera alternativa, los usuarios pueden acceder a la tienda a través del sitio de Receiver para Web, que permite que los usuarios accedan a sus escritorios y aplicaciones a través de una página Web. De forma predeterminada con tiendas no autenticadas, Citrix Receiver para Web muestra las aplicaciones en una jerarquía de carpetas que incluye una ruta de acceso al árbol de navegación. La URL de acceso a un sitio de Receiver para Web, utilizada para acceder a la nueva tienda, aparece al crearla.

Al crear una nueva tienda, la URL de servicios XenApp correspondiente se habilita de forma predeterminada. Los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados que ejecuten el Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a las tiendas directamente mediante la URL de servicios XenApp para la tienda. La URL de servicios XenApp tiene el formato http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, donde serveraddress es el nombre de dominio completo del servidor o entorno de equilibrio de carga de la implementación de StoreFront y storename es el nombre especificado para la tienda en el paso 3.

Nota: En configuraciones de StoreFront donde el archivo web.config se ha configurado con el parámetro LogoffAction=”terminate", las sesiones de CitrixReceiver para Web que acceden a esta tienda no autenticada no finalizarán. Normalmente, el archivo web.config se encuentra en C:\inetpub\wwwroot\Citrix\storename\, donde storename es el nombre especificado para la tienda cuando fue creada. Para asegurarse de que estas sesiones finalizan correctamente, el servidor XenApp utilizado por esta tienda debe tener habilitada la opción Confiar en solicitudes XML, según se describe en *Configuración del puerto y del parámetro de confianza de Citrix XML Service*. en la documentación de XenApp y XenDesktop.

Exportación de archivos de aprovisionamiento de tiendas para los usuarios

Aug 14, 2017

Utilice las tareas Exportar archivo de aprovisionamiento multialmacén y Exportar archivo de aprovisionamiento con el fin de generar archivos que contengan datos de conexión para las tiendas, incluidas las implementaciones de NetScaler Gateway y las balizas configuradas para las tiendas. Ponga estos archivos a disposición de los usuarios para permitirles que configuren Citrix Receiver automáticamente con la información de las tiendas. Los usuarios también pueden obtener los archivos de aprovisionamiento de Citrix Receiver desde los sitios de Receiver para Web.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront.
2. Para generar un archivo de aprovisionamiento que contenga información para varias tiendas, en el panel Acciones, haga clic en Exportar archivo de aprovisionamiento multi-tienda y seleccione las tiendas que desee incluir en el archivo.
3. Haga clic en Exportar y guarde el archivo de aprovisionamiento con la extensión .cr en una ubicación adecuada de la red.

Anunciar y ocultar tiendas para los usuarios

Aug 14, 2017

Utilice la tarea Ocultar tienda para evitar que se muestren tiendas a los usuarios y, por tanto, que las puedan agregar a sus cuentas cuando configuren Citrix Receiver mediante la detección de cuentas basada en direcciones de correo electrónico o FQDN. Cuando crea una tienda, ésta se muestra de forma predeterminada como una opción para que los usuarios la agreguen a Citrix Receiver al detectarse la implementación de StoreFront que aloja la tienda. Ocultar una tienda no la hace inaccesible; los usuarios deben configurar Citrix Receiver con los datos de conexión de la tienda. Pueden hacerlo de forma manual, usando una URL de configuración o con un archivo de aprovisionamiento. Para volver a mostrar una tienda oculta, utilice la tarea Anunciar tienda.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Configurar parámetros de la tienda > Anunciar tienda**.
3. En la página **Anunciar almacén**, seleccione **Anunciar almacén** o **Ocultar almacén**.

Administración de los recursos disponibles en las tiendas

Aug 14, 2017

Utilice la tarea Administrar Controllers para agregar o quitar los recursos que proporcionan XenDesktop, XenApp y App Controller dentro de una tienda, y para modificar la información de los servidores que ofrecen esos recursos.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel Acciones, haga clic en Administrar Delivery Controllers.
3. En el cuadro de diálogo Administrar Delivery Controllers, haga clic en Agregar para incluir escritorios y aplicaciones de otra implementación de XenDesktop, XenApp o App Controller en la tienda. Para modificar la configuración de una implementación, seleccione la entrada de la lista de Delivery Controllers y haga clic en Modificar. Seleccione una entrada de la lista y haga clic en Quitar para detener los recursos proporcionados por la implementación que está disponible en la tienda.
4. En el cuadro de diálogo Agregar Controller o Modificar Controller, especifique un nombre que le ayude a identificar la implementación e indique si los recursos que quiere colocar en la tienda son proporcionados por XenDesktop, XenApp o AppController. En caso de implementaciones de App Controller, asegúrese de que el nombre especificado no contiene espacios.
5. Si quiere agregar información de los servidores XenDesktop o XenApp, continúe en el paso 6. Para que las aplicaciones que administra App Controller estén disponibles en la tienda, escriba el nombre o la dirección IP de un dispositivo virtual App Controller en el cuadro Servidor y especifique el puerto que StoreFront debe utilizar para las conexiones con App Controller. El puerto predeterminado es 443. Continúe en el paso 10.
6. Para que los escritorios y las aplicaciones que proporcionan XenDesktop o XenApp estén disponibles en la tienda, haga clic en Agregar para introducir el nombre o la dirección IP de un servidor. Dependiendo de cómo esté configurado el archivo web.config, cuando se especifican varios servidores se habilita el equilibrio de carga o la conmutación por error, según se indica en el cuadro de diálogo. De manera predeterminada, se configura el equilibrio de carga. Si configura conmutación por error, coloque las entradas de la lista por orden de prioridad para definir la secuencia de conmutación por error que desee. Para los sitios de XenDesktop, proporcione información de los Delivery Controllers. En el caso de las comunidades de XenApp, enumere los servidores que ejecutan Citrix XML Service. Para modificar el nombre o la dirección IP de un servidor, seleccione la entrada de la lista Servidores y haga clic en Modificar. Seleccione una entrada de la lista y haga clic en Quitar para que StoreFront deje de comunicarse con el servidor con el objetivo de enumerar los recursos disponibles para el usuario.
7. En la lista Tipo de transporte, seleccione el tipo de conexiones que debe utilizar StoreFront para las comunicaciones con los servidores.
   - Para enviar datos a través de conexiones sin cifrar, seleccione HTTP. Si selecciona esta opción, deberá definir su propia configuración para proteger las conexiones entre StoreFront y los servidores.
   - Para enviar datos a través de conexiones HTTP seguras mediante SSL (Secure Sockets Layer) o TLS (Transport Layer Security), seleccione HTTPS. Si selecciona esta opción para servidores de XenDesktop y XenApp, asegúrese de que Citrix XML Service esté configurado para compartir su puerto con Microsoft Internet Information Services (IIS) y que IIS esté configurado para admitir HTTPS.

- Para enviar datos a través de conexiones seguras a servidores XenApp y utilizar el Traspaso SSL para realizar la autenticación del host y el cifrado de datos, seleccione Traspaso SSL.

Nota: Si utiliza HTTPS o el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores, compruebe que los nombres de servidores que especificó en la lista Servidores coincidan exactamente (incluidas mayúsculas y minúsculas) con los nombres en los certificados para esos servidores.

8. Especifique el puerto que StoreFront debe utilizar para las conexiones con los servidores. El puerto predeterminado para las conexiones que utilizan HTTP y el Traspaso SSL es 80, y para las conexiones mediante HTTPS es 443. En el caso de los servidores de XenDesktop y XenApp, el puerto especificado debe ser el puerto usado por Citrix XML Service.
9. Si utiliza el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores de XenApp, especifique el puerto TCP del Traspaso SSL en el cuadro Puerto del Traspaso SSL. El puerto predeterminado es 443. Asegúrese de que todos los servidores que ejecutan el Traspaso SSL estén configurados para escuchar en el mismo puerto.
10. Haga clic en Aceptar. Puede configurar las tiendas para que proporcionen recursos desde cualquier combinación de implementaciones de XenDesktop, XenApp y App Controller. Repita los pasos del 3 a 10, tantas veces como sea necesario, para agregar o modificar otras implementaciones de la lista de Delivery Controllers.

Administración del acceso remoto a las tiendas a través de NetScaler Gateway

Aug 14, 2017

Utilice la tarea Configurar parámetros de acceso remoto para configurar el acceso a las tiendas a través de NetScaler Gateway que se les otorga a los usuarios que se conectan desde redes públicas. El acceso remoto mediante NetScaler Gateway no se puede aplicar a tiendas no autenticadas.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel Acciones, haga clic en **Configurar parámetros de acceso remoto**.
3. En el cuadro de diálogo **Configurar** parámetros de acceso remoto, especifique si los usuarios que se conectan desde redes públicas pueden acceder a la tienda a través de NetScaler Gateway y la forma en que pueden hacerlo.
   - Para hacer que la tienda no esté disponible para los usuarios de redes públicas, asegúrese de dejar sin marcar la casilla **Habilitar acceso remoto**. Solo los usuarios locales de la red interna podrán acceder a la tienda.
   - Para habilitar el acceso remoto, marque la casilla **Habilitar acceso remoto**.
     - Para que estén disponibles solo los recursos entregados por la tienda en NetScaler Gateway, seleccione Sin túnel VPN. Los usuarios inician sesión directamente en NetScaler Gateway y no necesitan usar el NetScaler Gateway Plug-in.
     - Para que la tienda y otros recursos de la red interna estén disponibles a través de un túnel VPN SSL (Secure Sockets Layer), seleccione Túnel VPN completo. Los usuarios necesitan el NetScaler Gateway Plug-in para establecer el túnel VPN.

   Si no está habilitado, el método de autenticación PassThrough desde NetScaler Gateway se habilita automáticamente cuando se configura el acceso remoto a la tienda. Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.

4. Si habilitó el acceso remoto, seleccione en la lista de dispositivos NetScaler Gateway las implementaciones a través de las que los usuarios pueden acceder a la tienda. Las implementaciones previamente configuradas para esta y otras tiendas están disponibles y se pueden seleccionar de la lista. Si desea agregar otra implementación a la lista, haga clic en Agregar. De lo contrario, continúe en el paso 16.
5. En la página Parámetros generales, especifique un nombre para la implementación de NetScaler Gateway que ayude a los usuarios a identificarla.
   Los usuarios verán el nombre simplificado que especifique en Citrix Receiver, de modo que debe incluir la información relevante en el nombre para ayudarles a identificarlo y decidir si desean utilizar esa implementación o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de NetScaler Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.

6. Escriba la URL del servidor virtual o punto de entrada de usuarios (para Access Gateway 5.0) para la implementación. Especifique la versión de producto utilizada en la implementación.
   El nombre de dominio completo (FQDN) para la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de NetScaler Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual

de NetScaler Gateway.

7. Si va a agregar una implementación de Access Gateway 5.0, continúe en el paso 9. De lo contrario, especifique la dirección IP de subred del dispositivo NetScaler Gateway, si es necesario. Se necesita una dirección IP de subred para los dispositivos Access Gateway 9.3. Esta dirección es optativa si se trata de versiones más recientes de producto.
   La dirección de subred es la dirección IP que NetScaler Gateway utiliza para representar el dispositivo de usuario cuando se comunica con los servidores de la red interna. También puede ser la dirección IP asignada del dispositivo NetScaler Gateway. Cuando está especificada, StoreFront utiliza la dirección IP de subred para verificar que las solicitudes entrantes provienen de un dispositivo de confianza.

8. Si desea agregar un dispositivo con NetScaler Gateway 11, NetScaler Gateway 10.1, Access Gateway 10, o Access Gateway 9.3, seleccione en la lista Tipo de inicio de sesión el método de autenticación configurado en el dispositivo para los usuarios de Citrix Receiver.
   La información que proporcione sobre la configuración de su dispositivo NetScaler Gateway se agrega al archivo de aprovisionamiento para la tienda. Esto permite que Citrix Receiver envíe la solicitud de conexión pertinente al comunicarse con el dispositivo por primera vez.

   - Si es necesario que los usuarios introduzcan sus credenciales de dominio de Microsoft Active Directory, seleccione Dominio.
   - Si es necesario que los usuarios introduzcan un código de token obtenido de un token de seguridad, seleccione Token de seguridad.
   - Si es necesario que los usuarios introduzcan sus credenciales de dominio y un código de token obtenido de un token de seguridad, seleccione Dominio y token de seguridad.
   - Si es necesario que los usuarios introduzcan una contraseña de un solo uso enviada por mensaje de texto, seleccione Autenticación SMS.
   - Si es necesario que los usuarios presenten una tarjeta inteligente e introduzcan un PIN, seleccione Tarjeta inteligente.

   Si configura la autenticación con tarjeta inteligente con un método secundario de autenticación (al que los usuarios puedan recurrir en caso de tener problemas con su tarjeta inteligente), seleccione el método secundario de autenticación en la lista Alternativa a tarjeta inteligente. Continúe en el paso 10.

9. Para agregar una implementación de Access Gateway 5.0, indique si el punto de entrada del usuario está alojado en un dispositivo independiente o en un servidor de Access Controller que forma parte de un clúster. Si desea agregar un clúster, haga clic en Siguiente y continúe en el paso 11.
10. Si desea configurar StoreFront para NetScaler Gateway 11, NetScaler Gateway 10.1, Access Gateway 10, Access Gateway 9.3 o un único dispositivo Access Gateway 5.0, complete la URL del servicio de autenticación de NetScaler Gateway en el cuadro URL de respuesta. StoreFront anexa automáticamente la parte estándar de la dirección URL. Haga clic en Siguiente y continúe en el paso 13.
    Escriba la URL internamente accesible del dispositivo. StoreFront se comunica con el servicio de autenticación de NetScaler Gateway para verificar que las solicitudes recibidas de NetScaler Gateway provienen de ese dispositivo.

11. Para configurar StoreFront para un clúster de Access Gateway 5.0, enumere en la página Dispositivos las direcciones IP o FQDN de los dispositivos del clúster y haga clic en Siguiente.
12. En la página Habilitar autenticación silenciosa, enumere las direcciones URL para el servicio autenticación que se ejecuta en los servidores de Access Controller. Agregue direcciones URL de varios servidores para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Haga clic en Siguiente.
    StoreFront utiliza el servicio de autenticación para realizar la autenticación de los usuarios remotos para que no necesiten volver a introducir sus credenciales cuando accedan a las tiendas.

13. En todas las implementaciones, para que los recursos proporcionados por XenDesktop o XenApp estén disponibles en la tienda, enumere en la página Secure Ticket Authority (STA) las direcciones URL de los servidores que ejecutan STA. Introduzca direcciones URL vinculadas a varios STA para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error.
    El STA está alojado en servidores XenDesktop y XenApp. Emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.

14. Si desea que XenDesktop y XenApp mantengan abiertas las sesiones desconectadas mientras Citrix Receiver intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y desea asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tiquets de dos STA, si están disponibles.
    Cuando la casilla Solicitar tiquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tiquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA no está disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.

15. Haga clic en Crear para agregar la implementación de NetScaler Gateway a la lista del cuadro de diálogo Parámetros de acceso remoto.
16. Repita todos los pasos del 4 al 15, según sea necesario, para agregar más implementaciones de NetScaler Gateway a la lista de dispositivos NetScaler Gateway. Si habilita el acceso a través de varias implementaciones mediante la selección de más de una entrada de la lista, especifique la implementación predeterminada que se utilizará para acceder a la tienda.

Integración de las aplicaciones de Citrix Online en las tiendas

Aug 14, 2017

> ## Nota
>
> Desde StoreFront 3.12, esta función no puede configurarse en la consola de administración de StoreFront.Si actualiza a StoreFront 3.12, podrá seguir usando esta característica. Para cambiar la configuración, use el cmdlet de PowerShell llamado Update-DSGenericApplications.
>
> Para obtener información sobre cómo configurar esta función desde la consola de administración de StoreFront en las versiones anteriores, consulte el artículo de StoreFront 3.11 Integración con Citrix Online.

Update-DSGenericApplications

NOMBRE
Update-DSGenericApplications

RESUMEN
Actualiza los parámetros genéricos de aplicaciones para un servicio de tienda.

SINTAXIS

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

DESCRIPCIÓN

Cmdlet utilizado para actualizar la funcionalidad genérica (Citrix Online) del servicio de tienda.

Configuración de dos tiendas de StoreFront para compartir un almacén de datos de suscripción común

Aug 14, 2017

A partir de la versión 2.0, StoreFront ya no utiliza una base de datos SQL para mantener los datos de suscripción. Citrix ha reemplazado dicha base de datos SQL por un almacén de datos de Windows que no requiere ninguna configuración adicional cuando StoreFront se instala por primera vez. El programa de instalación instala el almacén de datos de Windows de forma local en todos los servidores StoreFront. En los entornos de grupos de servidores StoreFront, cada servidor también mantiene una copia de los datos de suscripción que emplea su tienda. Estos datos se propagan a otros servidores para el mantenimiento de las suscripciones de los usuarios en todo el grupo. De forma predeterminada, StoreFront crea un almacén de datos único para cada tienda. Cada almacén de datos de suscripción se actualiza de forma independiente con respecto a otras tiendas.

Es común que los administradores configuren StoreFront con dos tiendas diferentes allá donde se necesiten diferentes parámetros de configuración. Una de las tiendas es para el acceso externo a recursos a través de NetScaler Gateway y la otra es para el acceso interno a través de la red LAN de la organización. Puede configurar tiendas "externas" e "internas" para compartir un mismo almacén de datos de suscripción con solo realizar un pequeño cambio en el archivo web.config de la tienda.

En el escenario predeterminado con dos tiendas y sus almacenes de datos de suscripción correspondientes, los usuarios deben suscribirse al mismo recurso dos veces. Si se configuran ambas tiendas para compartir una misma base de datos de suscripción, puede mejorar y simplificar la experiencia de los usuarios móviles cuando estos acceden al mismo recurso desde dentro o desde fuera de la red corporativa. Con un almacén de datos de suscripción compartido, no importa si usan la tienda "externa" o la "interna" cuando se suscriben por primera vez a un nuevo recurso.

- Cada tienda tiene un archivo web.config ubicado en C:\inetpub\wwwroot\citrix\<storename>.
- Cada archivo web.config contiene un punto final de cliente para el servicio de almacenes de suscripción.

StoreName>" authenticationMode="windows" transferMode="Streamed">
Los datos de suscripción de cada almacén se encuentran en:

C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
Para que dos tiendas compartan un almacén de datos de suscripción, solo necesita apuntar una tienda al punto final del servicio de suscripción de la otra tienda. Si se trata de la implementación de un grupo de servidores, todos los servidores tienen definidos pares idénticos de tiendas y copias idénticas del almacén de datos que comparten.

Nota: Los Controllers de XenApp, XenDesktop y AppC configurados en cada almacén deben coincidir exactamente; de lo contrario, puede haber incoherencias al comparar los conjuntos de suscripciones a recursos de los almacenes. El uso compartido de un almacén de datos solo está respaldado cuando las dos tiendas se encuentran en el mismo servidor StoreFront o en la misma implementación de un grupo de servidores.

Puntos finales de los almacenes de datos de suscripción de StoreFront

1. En una implementación de StoreFront, abra el archivo web.config del almacén externo con el Bloc de notas y busque clientEndpoint. Por ejemplo:
   External" authenticationMode="windows" transferMode="Streamed">
2. Cambie el punto final de la tienda external para que coincida con internal:
   Internal" authenticationMode="windows" transferMode="Streamed">

3. Si está usando un grupo de servidores StoreFront, propague a todos los nodos del grupo los cambios que haya hecho en el archivo web.config del nodo principal.

Ahora, ambas tiendas están configuradas para compartir el almacén de datos de suscripción de la tienda interna.

Parámetros avanzados de las tiendas

Aug 14, 2017

Puede configurar propiedades avanzadas de las tiendas mediante la página Parámetros avanzados en Configurar parámetros de la tienda.

Tipo de resolución de direcciones

Permitir suavizado de fuentes

Permitir la reconexión de sesiones

Permitir la redirección de carpetas especiales

Periodo de sondeo de comprobación de estado en segundo plano

Duración del tiempo de espera de las comunicaciones

Tiempo de espera de la conexión

Habilitar enumeración mejorada

Habilitación de la agrupación de sockets

Filtrar recursos por palabras clave excluidas

Filtrar recursos por palabras clave incluidas

Filtrar recursos por tipo

Máximo de enumeraciones simultáneas

Mínimo de comunidades para la enumeración simultánea

Sobrescribir nombre de cliente ICA

Requerir coherencia de token

Intentos de comunicación con los servidores

Mostrar Desktop Viewer para clientes antiguos

Important

En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione una tienda en el panel central y, a continuación, seleccione **Configurar parámetros de la tienda**.
3. En la página **Configurar parámetros de la tienda**, seleccione **Parámetros avanzados**, seleccione la opción que quiere configurar, haga los cambios necesarios, y haga clic en **Aceptar**.

Tipo de resolución de direcciones

Utilice la tarea **Parámetros avanzados** para especificar el tipo de dirección que hay que solicitar al servidor. El valor predeterminado es DnsPort. En el menú desplegable **Tipo de resolución de direcciones** en **Parámetros avanzados**, seleccione una de las siguientes opciones:

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

Permitir suavizado de fuentes

Puede especificar si desea usar suavizado de fuentes para las sesiones HDX. El valor predeterminado es Activado.

Utilice la tarea **Parámetros avanzados**, marque la casilla **Permitir suavizado de fuentes**, y haga clic en **Aceptar**.

Permitir la reconexión de sesiones

Puede especificar si desea que las sesiones HDX puedan reconectarse. El valor predeterminado es Activado.

Utilice la tarea **Parámetros avanzados**, marque la casilla **Permitir la reconexión de sesiones** y haga clic en **Aceptar**.

Permitir la redirección de carpetas especiales

Utilice la tarea **Parámetros avanzados** para habilitar o inhabilitar la redirección de carpetas especiales. Si la redirección de carpetas especiales está configurada, los usuarios pueden asignar carpetas especiales de Windows del servidor a carpetas de sus equipos locales. El término "carpetas especiales" hace referencia a carpetas estándar de Windows, tales como las carpetas \Documentos y \Escritorio, que siempre se presentan del mismo modo, independientemente del sistema operativo.

Use la tarea **Parámetros avanzados**, marque o deje sin marcar la casilla **Permitir la redirección de carpetas especiales** según quiera habilitar o inhabilitar esta característica, y haga clic en **Aceptar**.

Periodo de sondeo de comprobación de estado en segundo plano

StoreFront ejecuta comprobaciones de estado periódicas en cada uno de los brokers de XenDesktop y servidores XenApp para reducir el impacto de disponibilidad intermitente de los servidores. El valor predeterminado es realizar una comprobación cada minuto (00:01:00). Utilice la tarea Parámetros avanzados, especifique el **Periodo de sondeo de comprobación de estado en segundo plano** y haga clic en **Aceptar** para controlar la frecuencia de las comprobaciones de estado.

Duración del tiempo de espera de las comunicaciones

De forma predeterminada, las solicitudes de StoreFront para un servidor que proporciona los recursos para una tienda tienen un tiempo de espera máximo de 30 segundos. El servidor se considera no disponible después de 1 intento de comunicación sin éxito. Utilice la tarea **Parámetros avanzados**, haga los cambios que desee en los valores de tiempo predeterminados y haga clic en **Aceptar** para cambiar estos parámetros.

Tiempo de espera de la conexión

Puede especificar cuántos segundos se debe esperar al establecer una conexión inicial con un Delivery Controller. El valor predeterminado es 6.

Utilice la tarea **Parámetros avanzados**, especifique los segundos de espera al establecer la conexión inicial y haga clic en **Aceptar**.

Habilitar enumeración mejorada

Puede habilitar o inhabilitar la comunicación en paralelo con los Delivery Controllers. El valor predeterminado es Activado.

Utilice la tarea **Parámetros avanzados**, marque o deje sin marcar la casilla **Habilitar enumeración mejorada**, y haga clic en **Aceptar.**

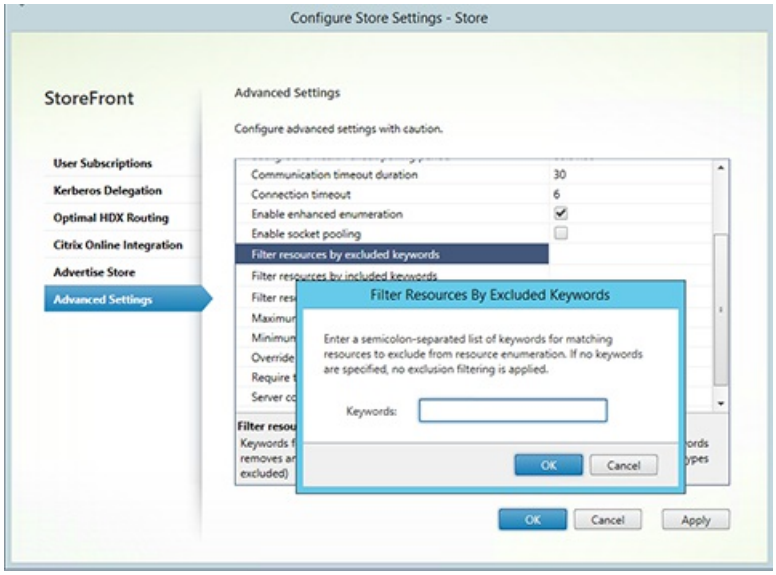
Habilitar la agrupación de sockets

De forma predeterminada, la agrupación de sockets está inhabilitada en las tiendas. Cuando la agrupación de sockets está habilitada, StoreFront mantiene una agrupación de sockets en lugar de crear un socket cada vez que se necesita uno y devolverlo al sistema operativo cuando se cierra la conexión. La habilitación de la agrupación de sockets mejora el rendimiento, especialmente para conexiones SSL. Para habilitar la agrupación de sockets, edite el archivo de configuración de la tienda. Utilice la tarea **Parámetros avanzados**, marque la casilla **Habilitar la agrupación de sockets** y haga clic en **Aceptar**.

Filtrar recursos por palabras clave excluidas

Puede filtrar los recursos utilizando palabras clave de exclusión. Cuando se especifican palabras clave de exclusión se quitan las palabras clave de inclusión previamente especificadas. El valor predeterminado es No filtrar (no se excluye ningún tipo de recurso).

Utilice la tarea **Parámetros avanzados**, seleccione **Filtrar recursos por palabras clave excluidas**, haga clic a su derecha, introduzca una lista de palabras clave separadas por punto y coma en el cuadro para introducir las palabras clave y haga clic en **Aceptar**.



Filtrar recursos por palabras clave incluidas

Puede filtrar los recursos utilizando palabras clave incluidas. Cuando se especifican palabras clave de inclusión se quitan las palabras clave de exclusión previamente especificadas. El valor predeterminado es No filtrar (no se excluye ningún tipo de recurso).

Utilice la tarea **Parámetros avanzados**, seleccione **Filtrar recursos por palabras clave incluidas**, haga clic a su derecha, introduzca una lista de palabras clave separadas por punto y coma en el cuadro para introducir las palabras clave y haga clic en **Aceptar**.

Filtrar recursos por tipo

Elija los tipos de recursos que se van a incluir en la enumeración de recursos. El valor predeterminado es No filtrar (se incluyen todos los tipos de recurso).

Utilice la tarea **Parámetros avanzados**, seleccione **Filtrar recursos por tipo**, haga clic a su derecha, elija los tipos de recursos para incluir en la enumeración y haga clic en **Aceptar**.

Máximo de enumeraciones simultáneas

Especifique la cantidad máxima de solicitudes simultáneas para enviar a diferentes de los Delivery Controllers. El valor predeterminado es 0 (no hay límite).

Utilice la tarea **Parámetros avanzados**, seleccione **Máximo de enumeraciones simultáneas**, introduzca el número y haga clic en **Aceptar**.

Mínimo de comunidades para la enumeración simultánea

Especifique el número mínimo de Delivery Controllers para realizar enumeraciones en paralelo. El valor predeterminado es 3.

Utilice la tarea **Parámetros avanzados**, seleccione **Mínimo de comunidades para la enumeración simultánea**, introduzca el número y haga clic en **Aceptar**.

Sobrescribir nombre de cliente ICA

Reemplaza el parámetro de nombre del cliente en el archivo .ica de inicio con un ID generado por Citrix Receiver para Web. Cuando está inhabilitado, Citrix Receiver especifica el nombre del cliente. El valor predeterminado es Desactivado.

Utilice la tarea **Parámetros avanzados**, marque la casilla **Sobrescribir nombre de cliente ICA**, y haga clic en **Aceptar**.

Requerir coherencia de token

Cuando está habilitado, StoreFront aplica uniformidad entre la puerta de enlace que se usa para autenticar y la puerta de enlace que se usa para acceder a la tienda. Si los valores no son coherentes, los usuarios deben volver a autenticarse. Es necesario habilitar esta opción para aplicar Smart Access. El valor predeterminado es Activado.

Utilice la tarea **Parámetros avanzados**, marque la casilla **Requerir coherencia de token**, y haga clic en **Aceptar**.

Intentos de comunicación con los servidores

Especifique cuántos intentos fallidos de comunicación con un Delivery Controller pueden tener lugar antes de marcarlo como no disponible. El valor predeterminado es 1.

Utilice la tarea **Parámetros avanzados**, seleccione **Intentos de comunicación con los servidores**, introduzca el número y haga clic en **Aceptar**.

Mostrar Desktop Viewer para clientes antiguos

Especifique si desea mostrar la ventana y la barra de herramientas de Citrix Desktop Viewer cuando los usuarios acceden a sus escritorios desde clientes antiguos. El valor predeterminado es Desactivado.

Utilice la tarea **Parámetros avanzados**, marque la casilla **Mostrar Desktop Viewer para clientes antiguos**, y haga clic en **Aceptar**.

Administración de un sitio de Citrix Receiver para Web

Aug 14, 2017

Citrix Receiver para Web permite acceder a aplicaciones, datos y escritorios de forma sencilla y segura desde una amplia gama de dispositivos. Utilice StoreFront para configurar la selección de aplicaciones de Citrix Receiver para Web.

Utilice la consola de administración de StoreFront para llevar a cabo tareas relacionadas con Citrix Receiver para Web:

Creación de un sitio de Citrix Receiver para Web	Cree sitios de Receiver para Web, que permiten a los usuarios acceder a tiendas a través de una página Web.
Configuración de sitios de Citrix Receiver para Web	Modifique la configuración de los sitios de Receiver para Web.
Configuración de respaldo para la experiencia unificada de Citrix Receiver	StoreFront admite tanto la experiencia de usuario clásica como la unificada. La experiencia unificada ofrece una experiencia de usuario en HTML5 que se puede administrar de forma centralizada
Creación y administración de aplicaciones destacadas	Cree grupos de aplicaciones destacadas de productos, relacionadas o pertenecientes a una categoría específica, para los usuarios finales.
Configuración del control del espacio de trabajo	El control del espacio de trabajo permite que las aplicaciones sigan disponibles para los usuarios cuando estos cambian de dispositivo.
Configuración del uso de las pestañas del explorador Web con Citrix Receiver para HTML5	Cuando los usuarios inician recursos con Citrix Receiver para HTML5 a partir de accesos directos, especifique si el escritorio o la aplicación reemplazan el sitio de Citrix Receiver para Web en la pestaña existente del explorador en vez de aparecer en una nueva pestaña.
Configuración de la duración del tiempo de espera de las comunicaciones y de los reintentos	De forma predeterminada, el tiempo de espera de las solicitudes de un sitio de Citrix Receiver para Web para la tienda asociada se agota pasados tres minutos. La tienda se considera no disponible después de un intento de comunicación sin éxito.Puede cambiar el parámetro predeterminado, si lo desea.

Creación de un sitio de Citrix Receiver para Web

Aug 14, 2017

Utilice la tarea Crear sitio Web para agregar sitios de Receiver para Web, los cuales permiten que los usuarios accedan a las tiendas a través de una página Web.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione la tienda para la que quiere crear el sitio de Citrix Receiver para Web, y en el panel Acciones, haga clic en Administrar sitios de Receiver para Web.
3. Haga clic en **Agregar** para crear un nuevo sitio de Citrix Receiver para Web. Especifique la dirección URL en el cuadro Ruta del sitio Web y haga clic en **Siguiente**.
4. Seleccione la experiencia de Citrix Receiver y haga clic en **Siguiente**.
5. Elija un método de autenticación, haga clic en Crear y, a continuación, una vez que se haya creado un sitio, haga clic en Finalizar.
   Aparecerá la URL para que los usuarios accedan al sitio de Citrix Receiver para Web. Para obtener más información sobre cómo modificar los parámetros de los sitios de Citrix Receiver para Web, consulte Configuración de sitios de Citrix Receiver para Web.

De forma predeterminada, cuando un usuario accede a un sitio de Receiver para Web desde un equipo con Windows o Mac OS X, el sitio intenta determinar si Citrix Receiver está instalado en el dispositivo de usuario. Si no se detecta Citrix Receiver, se solicita al usuario que descargue e instale, del sitio Web de Citrix, la versión de Citrix Receiver correspondiente a su plataforma. Para obtener más información sobre cómo modificar este comportamiento, consulte Inhabilitación de la detección y la implementación de Citrix Receiver.

La configuración predeterminada de los sitios de Receiver para Web requiere que los usuarios instalen una versión compatible de Citrix Receiver para acceder a sus escritorios y aplicaciones. Sin embargo, puede habilitar Receiver para HTML5 en los sitios de Receiver para Web. De este modo, los usuarios tendrán acceso a los recursos aunque no puedan instalar Citrix Receiver. Para obtener más información, consulte Configuración de sitios de Citrix Receiver para Web.

Configuración de sitios de Citrix Receiver para Web

Aug 14, 2017

Los sitios de Citrix Receiver para Web permiten a los usuarios acceder a tiendas a través de una página Web. Las tareas siguientes permiten modificar los parámetros de los sitios de Citrix Receiver para Web. Algunos de los parámetros avanzados solo pueden cambiarse mediante la edición de los archivos de configuración del sitio. Para obtener más información, consulte Configuración de los sitios de Citrix Receiver para Web mediante los archivos de configuración.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Elección de métodos de autenticación

Utilice la tarea Métodos de autenticación si quiere asignar métodos de autenticación a usuarios que se conecten al sitio de Citrix Receiver para Web. Esta acción le permite especificar un subconjunto de métodos de autenticación para cada sitio de Receiver para Web.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront. A continuación, seleccione la tienda que quiera modificar en el panel de resultados.
3. En el panel Acciones, haga clic en **Administrar sitios de Receiver para Web**, haga clic en **Configurar**, y elija **Métodos de autenticación** para especificar los métodos de acceso que quiere habilitar para los usuarios.
   - Seleccione la casilla Nombre de usuario y contraseña para habilitar la autenticación explícita. Los usuarios introducen sus credenciales cuando acceden a sus tiendas.
   - Marque la casilla **Autenticación SAML** para habilitar la integración con proveedores de identidades SAML. Los usuarios se autentican en un proveedor de identidades y su sesión se inicia automáticamente cuando acceden a sus tiendas. Desde el menú desplegable Parámetros:
     - Seleccione **Proveedor de identidades** para configurar la confianza con el proveedor de identidades.
     - Seleccione **Proveedor de servicios** para configurar la confianza con el proveedor de servicios. El proveedor de identidades necesita esta información.
   - Marque la casilla PassThrough de dominio para habilitar la autenticación PassThrough de las credenciales de dominio de Active Directory desde los dispositivos de los usuarios. Los usuarios realizan la autenticación en los equipos unidos a un dominio de Windows y su sesión se inicia automáticamente cuando acceden a las tiendas. Para poder usar esta opción, la autenticación PassThrough debe estar habilitada cuando se instala Citrix Receiver para Windows en los dispositivos de los usuarios. Tenga en cuenta que la autenticación PassThrough de dominios en Citrix Receiver para Web está limitada a sistemas operativos Windows que utilicen Chrome, Firefox, Internet Explorer y Edge.
   - Marque la casilla Tarjeta inteligente para habilitar la autenticación con tarjeta inteligente. Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a las tiendas.
   - Marque la casilla PassThrough desde NetScaler Gateway para habilitar la autenticación PassThrough desde NetScaler Gateway. Los usuarios se autentican en NetScaler Gateway y su sesión se inicia automáticamente cuando acceden a sus tiendas.
4. Una vez seleccionado el método de autenticación, haga clic en Aceptar.
   Para obtener más información acerca de la modificación de los parámetros de los métodos de autenticación, consulte Configuración del servicio de autenticación.

Cómo agregar accesos directos a recursos en otros sitios Web

Utilice la tarea Agregar accesos directos a sitios Web para proporcionar a los usuarios acceso inmediato a escritorios y aplicaciones desde sitios Web alojados en la red interna. Debe generar direcciones URL para los recursos disponibles a través del sitio de Citrix Receiver para Web e insertar estos enlaces en los sitios Web. Los usuarios hacen clic en un enlace y se les redirige al sitio de Receiver para Web, donde deben iniciar sesión si todavía no lo han hecho. El sitio de Receiver para Web inicia automáticamente el recurso. En el caso de las aplicaciones, los usuarios también se suscriben a ellas si no lo han hecho anteriormente.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un sitio.
3. En el panel **Acciones** , haga clic en **Administrar sitios de Receiver para Web**, haga clic en **Configurar**, y elija **Accesos directos a sitios Web**.
4. Haga clic en **Agregar** para introducir la dirección URL del sitio Web donde va a colocar los accesos directos. Las direcciones URL deben especificarse con el formato http[s]://hostname[:port], donde hostname es el nombre de dominio completo del host del sitio Web y port es el puerto utilizado para la comunicación con el host, si el puerto predeterminado para el protocolo no está disponible. Las rutas a las páginas específicas del sitio Web no son necesarias. Para modificar una URL, seleccione la entrada de la lista Sitios Web y haga clic en Modificar. Seleccione una entrada de la lista y haga clic en Quitar para eliminar la URL de un sitio Web en el que ya no quiera alojar accesos directos a los recursos disponibles a través del sitio de Citrix Receiver para Web.
5. Haga clic en Obtenga accesos directos y, a continuación, haga clic en Guardar cuando se le solicite que guarde los cambios de configuración.
6. Inicie sesión en el sitio de Citrix Receiver para Web y copie las direcciones URL requeridas en el sitio Web.

Definición del tiempo de espera de las sesiones

De forma predeterminada, las sesiones de usuario de los sitios de Citrix Receiver para Web se cierran automáticamente después de 20 minutos de inactividad. Cuando una sesión caduca, los usuarios pueden continuar utilizando cualquier aplicación o escritorio que ya esté en ejecución, pero deben volver a iniciar sesión para acceder a las funciones de los sitios de Citrix Receiver para Web, como la suscripción a aplicaciones.

Utilice la tarea Tiempo de espera de la sesión en la pantalla **Administrar sitios de Receiver para Web** para cambiar el valor de tiempo de espera de la sesión.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo y, en el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web**, haga clic en **Configurar** y elija **Parámetros de la sesión**. Puede especificar minutos y horas para el **Tiempo de espera de la sesión**. El valor mínimo para todos los intervalos de tiempo es 1. El valor máximo equivale a 1 año para cada intervalo de tiempo.

Cómo especificar diferentes vistas de aplicaciones y escritorios

Use la tarea **Vista de aplicaciones y escritorios en Receiver para Web** en **Administrar sitios de Receiver para Web** para cambiar este parámetro.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo y, en el panel **Acciones**, haga clic en Administrar sitios de Receiver para Web, haga clic en **Configurar** y elija **Parámetros de interfaz de cliente**.
3. En los menús desplegables **Seleccionar vista** y **Vista predeterminada**, seleccione las vistas que quiera mostrar.

Para habilitar la vista de carpetas:

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo y, en el panel **Acciones** , haga clic en **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.
3. Seleccione **Parámetros avanzados** y marque la casilla **Habilitar vista de carpetas**.

Cómo dejar de ofrecer archivos de aprovisionamiento a los usuarios

De forma predeterminada, los sitios de Citrix Receiver para Web ofrecen archivos de aprovisionamiento que permiten que los usuarios puedan configurar automáticamente Citrix Receiver para la tienda asociada. Los archivos de aprovisionamiento contienen los datos de conexión para la tienda que proporciona los recursos en el sitio, incluidos los detalles de las implementaciones de NetScaler Gateway y las balizas configuradas para la tienda.

Utilice la tarea **Habilitar configuración de Receiver** en la pantalla **Administrar sitios de Receiver para Web** para cambiar el valor de tiempo de espera de la sesión.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo y, en el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web**, haga clic en **Configurar** y elija **Parámetros de interfaz de cliente**.
3. Seleccione **Habilitar configuración de Receiver**.

Configuración del comportamiento del sitio para los usuarios sin Citrix Receiver

Utilice la tarea **Implementar Citrix Receiver** para configurar el comportamiento de un sitio de Citrix Receiver para Web cuando un usuario de Windows o Mac OS X que no tiene instalado Citrix Receiver acceda al sitio. De forma predeterminada, los sitios de Citrix Receiver para Web intentan detectar automáticamente si Citrix Receiver está instalado cuando se accede a ellos desde equipos con Windows o Mac OS X.

Si no se detecta Citrix Receiver, se solicita al usuario que descargue e instale la versión de Citrix Receiver correspondiente a su plataforma. La ubicación de descarga predeterminada es el sitio Web de Citrix, pero también puede, en su lugar, copiar los archivos de instalación al servidor StoreFront y proporcionar a los usuarios estos archivos locales.

Para los usuarios que no pueden instalar Citrix Receiver, puede habilitar Citrix Receiver para HTML5 en los sitios de Citrix Receiver para Web. Citrix Receiver para HTML5 permite que los usuarios puedan acceder a escritorios y aplicaciones directamente en exploradores Web compatibles con HTML5 sin necesidad de instalar Citrix Receiver. Se admiten tanto las conexiones de la red interna como las conexiones a través de NetScaler Gateway. Sin embargo, si se trata de conexiones desde la red interna, Citrix Receiver para HTML5 solo permite el acceso a los recursos proporcionados por productos específicos. Además, se necesitan versiones específicas de NetScaler Gateway para habilitar las conexiones desde fuera de la red corporativa. Para obtener más información, consulte Requisitos de infraestructura.

De manera predeterminada, el acceso a través de Citrix Receiver para HTML5 para los recursos proporcionados por XenDesktop y XenApp se encuentra inhabilitado para los usuarios locales de la red interna. Para habilitar el acceso local a escritorios y aplicaciones mediante Citrix Receiver para HTML5, debe habilitar la directiva Conexiones de WebSockets en los servidores XenDesktop y XenApp. XenDesktop y XenApp utilizan el puerto 8008 para las conexiones de Citrix Receiver para HTML5. Asegúrese de que los firewalls y otros dispositivos de red permitan el acceso a este puerto. Para obtener más información, consulte Configuraciones de directiva de WebSockets.

Solo se puede utilizar Citrix Receiver para HTML5 con Internet Explorer en conexiones HTTP. Para utilizar Citrix Receiver para HTML5 con Mozilla Firefox con conexión HTTPS, los usuarios deben escribir about:config en la barra de direcciones de Firefox y establecer la preferencia **network.websocket.allowInsecureFromHTTPS** en **true**.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un sitio. En el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.
3. Elija **Implementar Citrix Receiver** y especifique la respuesta del sitio de Citrix Receiver para Web cuando no pueda detectarse Citrix Receiver en el dispositivo del usuario.

- Si quiere que el sitio solicite al usuario que descargue e instale la versión de Citrix Receiver correspondiente a su plataforma, seleccione **Instalar localmente**. Los usuarios deben instalar Citrix Receiver para acceder a escritorios y aplicaciones a través del sitio.
  - Si selecciona **Permitir que los usuarios descarguen el plug-in de HDX Engine**, Citrix Receiver para Web permite que el usuario descargue e instale Citrix Receiver en el cliente del usuario final si Citrix Receiver no está disponible en él.
  - Si selecciona **Actualizar el plug-in al iniciar sesión**, Citrix Receiver para Web actualiza el cliente Citrix Receiver cuando el usuario inicia una sesión. Para habilitar esta función, asegúrese de que los archivos de Citrix Receiver están disponibles en el servidor StoreFront.
  - Seleccione un origen de archivos en el menú desplegable.
- Si quiere que el sitio solicite al usuario que descargue e instale Citrix Receiver pero que recurra a Citrix Receiver para HTML5 si Citrix Receiver no puede instalarse, seleccione **Usar Citrix Receiver para HTML5 si el Receiver local no está disponible**. A los usuarios sin Citrix Receiver se les solicitará que descarguen e instalen Citrix Receiver cada vez que inicien sesión en el sitio.
- Si quiere que el sitio permita el acceso a los recursos a través de Citrix Receiver para HTML5 sin solicitar al usuario que descargue e instale Citrix Receiver, seleccione **Usar siempre Receiver para HTML5**. Con esta opción seleccionada, los usuarios siempre acceden a los escritorios y aplicaciones del sitio a través de Citrix Receiver para HTML5, siempre que utilicen un explorador compatible con HTML5. Los usuarios que no tienen un explorador compatible con HTML5 tienen que instalar el Citrix Receiver nativo.

Cómo ofrecer archivos de instalación de Citrix Receiver en el servidor

De forma predeterminada, cuando un usuario accede a un sitio de Citrix Receiver para Web desde un equipo con Windows o Mac OS X, el sitio intenta determinar si Citrix Receiver está instalado en el dispositivo de usuario. Si no se detecta Citrix Receiver, se solicita al usuario que descargue e instale, del sitio Web de Citrix, la versión de Citrix Receiver correspondiente a su plataforma.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un sitio. En el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.
3. Elija **Implementar Citrix Receiver** y **Archivos de origen de Receiver** y busque los archivos de instalación.

Ejecutar el símbolo del sistema para instalar Citrix Receiver después de iniciar sesión

Antes de iniciar la sesión en StoreFront, Citrix Receiver para Web solicita un usuario la instalación de la versión más reciente de Citrix Receiver, si Citrix Receiver aún no está instalado en el equipo del usuario (para usuarios de Internet Explorer, Firefox y Safari) o la primera vez que el usuario visita el sitio (en el caso de los usuarios de Chrome). Según la configuración, el mensaje también puede indicar si la instalación de Citrix Receiver que tiene el usuario se puede actualizar.

Puede configurar Citrix Receiver para Web para que muestre este mensaje después de iniciar sesión en StoreFront.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.

2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione el sitio.
3. En el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.
4. Seleccione **Parámetros avanzados** y marque la casilla **Pedir la instalación de Citrix Receiver después de iniciar la sesión**.

Eliminación de sitios de Citrix Receiver para Web

Use **Administrar sitios de Receiver para Web** en el panel **Acciones** para eliminar un sitio de Citrix Receiver para Web. Al quitar un sitio, los usuarios ya no pueden usar esa página Web para acceder a la tienda.

Respaldo para la experiencia unificada de Citrix Receiver

Aug 14, 2017

StoreFront admite tanto la experiencia de usuario **clásica** como la **unificada**. Con la experiencia clásica, cada plataforma de Citrix Receiver es responsable de entregar su propia experiencia de usuario. La nueva experiencia unificada ofrece una experiencia de usuario HTML5 administrada de forma centralizada para todos los Citrix Receiver nativos y para Web. Se admite la personalización y la administración de grupos de aplicaciones destacadas.

Las tiendas creadas con esta versión de StoreFront utilizan la experiencia unificada de forma predeterminada pero, para las actualizaciones, Citrix conserva la experiencia clásica de forma predeterminada. Para dar respaldo a la experiencia unificada, debe asociar una tienda de StoreFront a un sitio de Receiver para Web, y ese sitio debe estar configurado para usar la experiencia unificada.

Importante: La experiencia unificada no recibe respaldo si el sitio de Receiver para Web se agrega a la Zona restringida. Si es necesario agregar el sitio de Receiver para Web a la Zona restringida, configure la tienda para usar la experiencia clásica.

Utilice la consola de administración de StoreFront para llevar a cabo tareas relacionadas con Citrix Receiver para Web:

- Crear un sitio de Citrix Receiver para Web.
- Cambiar la experiencia del sitio de Citrix Receiver para Web.
- Seleccionar un sitio de Citrix Receiver para Web para asociarlo a la tienda.
- Personalizar la apariencia de Receiver.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

> ### Nota
>
> Si usa XenApp 6.x, no son compatibles las aplicaciones establecidas en **Distribuida por streaming al cliente** ni **Distribuida por streaming si es posible, si no, de otro servidor** con la experiencia unificada.

Creación de un sitio Web de Citrix Receiver para Web

Cada vez que se crea una nueva tienda, se crea automáticamente un sitio de Citrix Receiver para Web. También puede crear más sitios de Receiver para Web con este procedimiento.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Administrar sitios de Receiver para Web > Agregar y siga los pasos del asistente.

Cambio de la experiencia de Citrix Receiver

Puede seleccionar si un sitio de Citrix Receiver para Web entrega la experiencia **clásica** o **unificada**. Tenga en cuenta que habilitar la experiencia clásica inhabilita las personalizaciones avanzadas y la administración de grupos de aplicaciones

destacadas.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione la tienda que desea cambiar en el panel central y, a continuación, haga clic en **Administrar sitios de Receiver para Web** en el panel Acciones y, a continuación, haga clic en **Configurar**.
3. Seleccione **Experiencia de Receiver** y elija **Inhabilitar la experiencia clásica** o **Habilitar la experiencia clásica**.

Cómo seleccionar un sitio de Citrix Receiver para Web para asociarlo a la tienda

Cuando se crea una nueva tienda mediante StoreFront, también se crea automáticamente un sitio de Citrix Receiver para Web en modo unificado y se asocia a la tienda.Sin embargo, si se actualiza desde una versión anterior de StoreFront, de forma predeterminada, se conserva la experiencia clásica.

Para seleccionar un sitio de Citrix Receiver para Web y ofrecer la experiencia unificada para una tienda, debe tener al menos un sitio de Citrix Receiver para Web con la experiencia clásica inhabilitada.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione una tienda en el panel central y, a continuación, haga clic en **Configurar la experiencia unificada** en el panel **Acciones**. Solo los sitios Web que admiten la experiencia unificada (es decir, que tienen la experiencia clásica inhabilitada) se pueden usar como configuración predeterminada para la tienda. Si no ha creado todavía un sitio Web de Citrix Receiver para Web, aparecerá un mensaje con un enlace al asistente para crear un nuevo sitio Web de Receiver para Web. También puede cambiar un sitio de Receiver para Web existente en un sitio Web de Receiver para Web. Consulte Cambio de la experiencia de Citrix Receiver.
3. Si ya ha creado un sitio de Citrix Receiver para Web, elija **Configurar la experiencia unificada** para esta tienda y elija el sitio Web específico.

> ## Important
>
> Si cambia la experiencia unificada por la experiencia clásica en un sitio de Receiver para Web, esto puede afectar a los clientes Citrix Receiver nativos. Al cambiar la experiencia de vuelta a una experiencia unificada en este sitio de Receiver para Web no actualizará la experiencia para los clientes de los Citrix Receivers nativos. Debe restablecer la experiencia unificada en el nodo Tiendas de la consola de administración.

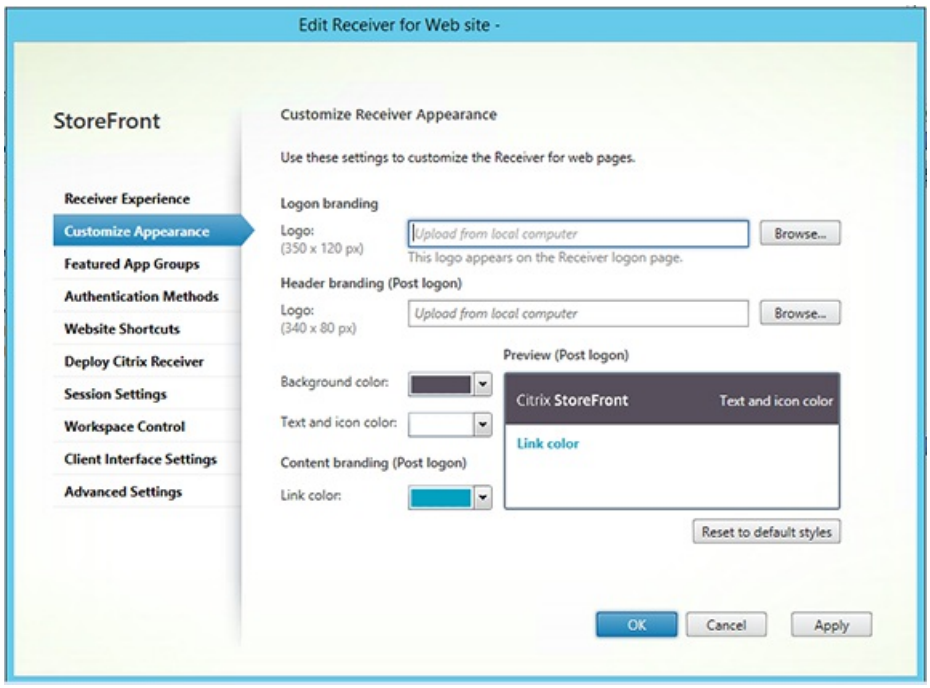
Personalización de la apariencia de Citrix Receiver

Para personalizar la apariencia de Citrix Receiver, el sitio Web de Citrix Receiver para Web debe tener la experiencia clásica de Citrix Receiver inhabilitada.

1. En la pantalla de **Inicio** o Aplicaciones de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel

Acciones, haga clic en **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.

3. Seleccione **Experiencia de Receiver** > **Inhabilitar la experiencia clásica**.
4. Seleccione **Personalizar apariencia** y realice las selecciones necesarias para personalizar cómo se muestra el sitio Web después de iniciar sesión.



Creación y administración de aplicaciones destacadas

Aug 14, 2017

Se pueden crear grupos de aplicaciones destacadas de productos, relacionadas o pertenecientes a una categoría específica, para los usuarios finales. Por ejemplo, puede crear un grupo de las aplicaciones destacadas del departamento de ventas que contenga las aplicaciones que se usen en ese departamento. Para definir aplicaciones destacadas en la consola de administración de StoreFront, puede valerse de los nombres de las aplicaciones, las palabras clave o las categorías de aplicaciones que se han definido en la consola de Studio.

Utilice la tarea Grupos de aplicaciones destacadas para agregar, modificar o quitar grupos de aplicaciones destacadas.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.
Tenga en cuenta que esta funcionalidad está disponible solamente cuando la experiencia clásica está inhabilitada.

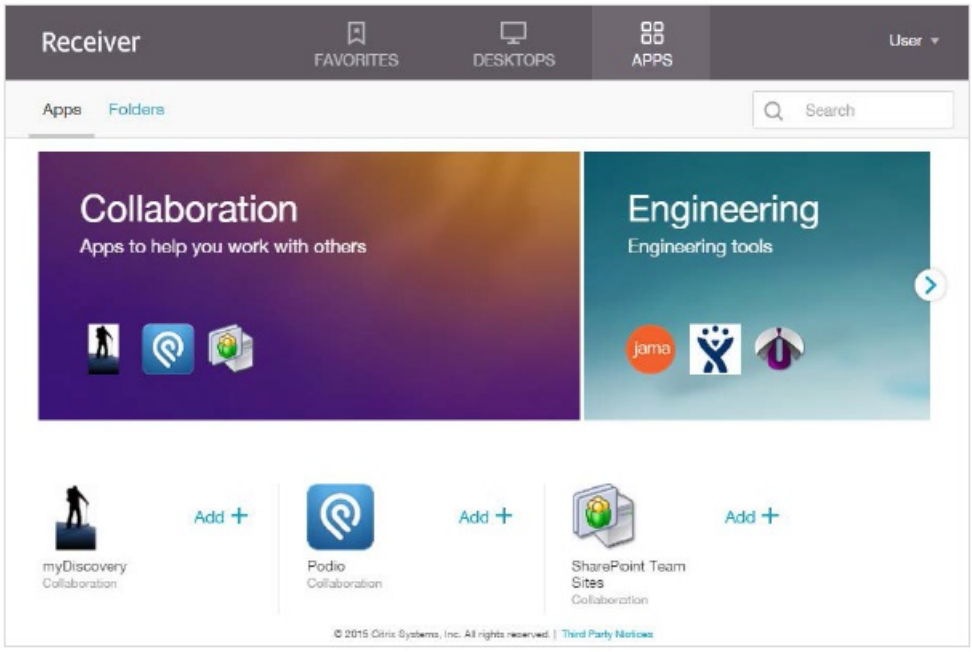
1. En la pantalla de **Inicio** o Aplicaciones de Windows, busque el icono de Citrix **StoreFront** y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.
3. Seleccione **Grupos de aplicaciones destacadas**.
4. En el cuadro de diálogo **Grupos de aplicaciones destacadas**, haga clic en **Crear** para definir un nuevo grupo de aplicaciones destacadas.
5. En el cuadro de diálogo **Crear grupo de aplicaciones destacadas**, especifique un nombre, una descripción (optativa) y un fondo, así como el método mediante el cual usted quiere definir los grupos de aplicaciones destacadas. Puede elegir entre palabras clave, nombres de las aplicaciones, o categoría de la aplicación. Después, haga clic en **Aceptar**.

Opción	Descripción
Palabras clave	Defina las palabras clave en Studio.
Categoría de aplicación	Defina la categoría de una aplicación en Studio.
Nombres de las aplicaciones	Use el nombre de las aplicaciones para definir el grupo de aplicaciones destacadas. Los nombres de todas las aplicaciones que coincidan con el nombre que contenga el cuadro de diálogo "Crear un grupo de aplicaciones destacadas" se incluyen en el grupo de aplicaciones destacadas. StoreFront no admite comodines en los nombres de las aplicaciones. En las coincidencias no se distinguen mayúsculas de minúsculas, aunque sí se distinguen palabras completas. Por ejemplo, si escribe Excel, StoreFront establece la correspondencia con una aplicación publicada llamada Microsoft Excel 2013. Sin embargo, si escribe Exc, no hay coincidencias.

Ejemplo:

Hemos creado dos grupos de aplicaciones destacadas:

- Collaboration: Creado con aplicaciones de la categoría **Collaboration** de Studio.
- Engineering: Creado dando un nombre al grupo de aplicaciones y especificando una colección de nombres de aplicaciones.



Configuración del control del espacio de trabajo

Aug 14, 2017

El control del espacio de trabajo permite que las aplicaciones sigan disponibles para los usuarios cuando estos cambian de dispositivo. Esto permite, por ejemplo, que los médicos, en los hospitales, se trasladen de una estación de trabajo a otra sin tener que reiniciar sus aplicaciones en cada dispositivo. El control del espacio de trabajo está habilitado de forma predeterminada para los sitios de Citrix Receiver para Web. Para inhabilitar o configurar el control del espacio de trabajo, modifique el archivo de configuración del sitio.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. En el panel izquierdo, seleccione **Tiendas** y en el panel Acciones, seleccione **Administrar sitios de Receiver para Web** y haga clic en **Configurar.**
3. Seleccione **Control del espacio de trabajo**.
4. Configure los parámetros predeterminados para el control del espacio de trabajo, que incluyen lo siguiente:

    Habilitación del control del espacio de trabajo

    Configuración de las opciones de reconexión de la sesión

    Especificación de la acción de cierre de sesión

Configuración del uso de las pestañas del explorador Web con Citrix Receiver para HTML5

Aug 14, 2017

De forma predeterminada, Citrix Receiver para HTML5 inicia los escritorios y las aplicaciones en una nueva pestaña del explorador. No obstante, cuando los usuarios inician recursos con Citrix Receiver para HTML5 a partir de accesos directos, el escritorio o la aplicación reemplazan el sitio de Citrix Receiver para Web en la pestaña existente del explorador en vez de aparecer en una nueva pestaña.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. En el panel izquierdo, seleccione **Tiendas** y en el panel Acciones, seleccione **Administrar sitios de Receiver para Web y haga clic en Configurar**.
3. Seleccione **Implementar Citrix Receiver**.
4. Seleccione **Usar siempre Receiver para HTML5** desde el menú desplegable **Opciones de implementación** y según la pestaña en la que se desee iniciar las aplicaciones, marque o deje sin marcar la opción **Iniciar aplicaciones en la misma pestaña que Receiver para Web**.

Configuración de la duración del tiempo de espera de las comunicaciones y de los reintentos

Aug 14, 2017

De forma predeterminada, el tiempo de espera de las solicitudes de un sitio de Citrix Receiver para Web para la tienda asociada se agota pasados tres minutos. La tienda se considera no disponible después de un intento de comunicación sin éxito. Utilice la tarea **Parámetros de la sesión** para cambiar los parámetros predeterminados.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione una tienda en el panel central y, a continuación, en el panel **Acciones**, seleccione **Administrar sitios de Receiver para Web** y haga clic en **Configurar.**
3. Seleccione **Parámetros de la sesión**, realice los cambios y haga clic en **Aceptar/Aplicar** para guardar los cambios.

Configuración del acceso de usuarios

Aug 14, 2017

Este artículo contiene la siguiente información:

> **Important**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Configuración del respaldo a conexiones a través de las direcciones URL de servicios XenApp

Utilice la tarea **Configurar respaldo de Servicios XenApp** para configurar el acceso a las tiendas a través de las direcciones URL de servicios XenApp. Los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados que ejecuten el Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a las tiendas directamente mediante la URL de servicios XenApp para la tienda. Al crear una nueva tienda, la URL de servicios XenApp correspondiente se habilita de forma predeterminada.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel **Acciones**, haga clic en **Configurar respaldo de servicios XenApp**.
3. Marque o desmarque la casilla **Habilitar respaldo de Servicios XenApp**, respectivamente, para habilitar o inhabilitar el acceso de los usuarios a la tienda mediante la URL de servicios XenApp que se muestra.
   La URL de los servicios XenApp para una tienda tiene el formato:
   http[s]://serveraddress/Citrix/storename/PNAgent/config.xml, donde *serveraddress* es el nombre de dominio completo del servidor o entorno de equilibrio de carga de la implementación de StoreFront y *storename* es el nombre especificado para la tienda cuando se creó.
4. Si habilita el respaldo de servicios XenApp, tiene la opción de especificar una tienda predeterminada en la implementación de StoreFront para los usuarios que cuentan con Citrix Online Plug-in.
   Especifique una tienda predeterminada, de modo que los usuarios puedan configurar Citrix Online Plug-in con la URL del servidor o la URL de equilibrio de carga de la implementación de StoreFront en lugar de la URL de servicios XenApp de una

tienda concreta.

Cómo habilitar o inhabilitar la reconexión de control del espacio de trabajo para todos los Citrix Receiver

El control del espacio de trabajo permite que las aplicaciones sigan a los usuarios cuando estos cambian de dispositivo. Esto permite, por ejemplo, que los médicos, en los hospitales, puedan trasladarse de una estación de trabajo a otra sin tener que reiniciar sus aplicaciones en cada dispositivo.

StoreFront contiene una configuración para inhabilitar la reconexión de control del espacio de trabajo en el servicio de tienda para todos los Citrix Receivers. Administre esta función mediante la consola de StoreFront o con PowerShell.

Uso de la consola de administración de StoreFront

1. En la pantalla de **Inicio** o Aplicaciones de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Configurar parámetros de la tienda**.
3. Seleccione **Parámetros avanzados** y marque o deje sin marcar la casilla **Permitir la reconexión de sesiones**.

Mediante PowerShell

Compruebe que ha cerrado la consola de administración. Ejecute el siguiente fragmento de código para importar los módulos de StoreFront de PowerShell:

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

Entonces, el comando de PowerShell **Set-DSAllowSessionReconnect** activa o desactiva la reconexión de control del espacio de trabajo.

Sintaxis

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

Por ejemplo, para desactivar la reconexión de control del espacio de trabajo en una tienda en /Citrix/Store, el siguiente comando configura la tienda:

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

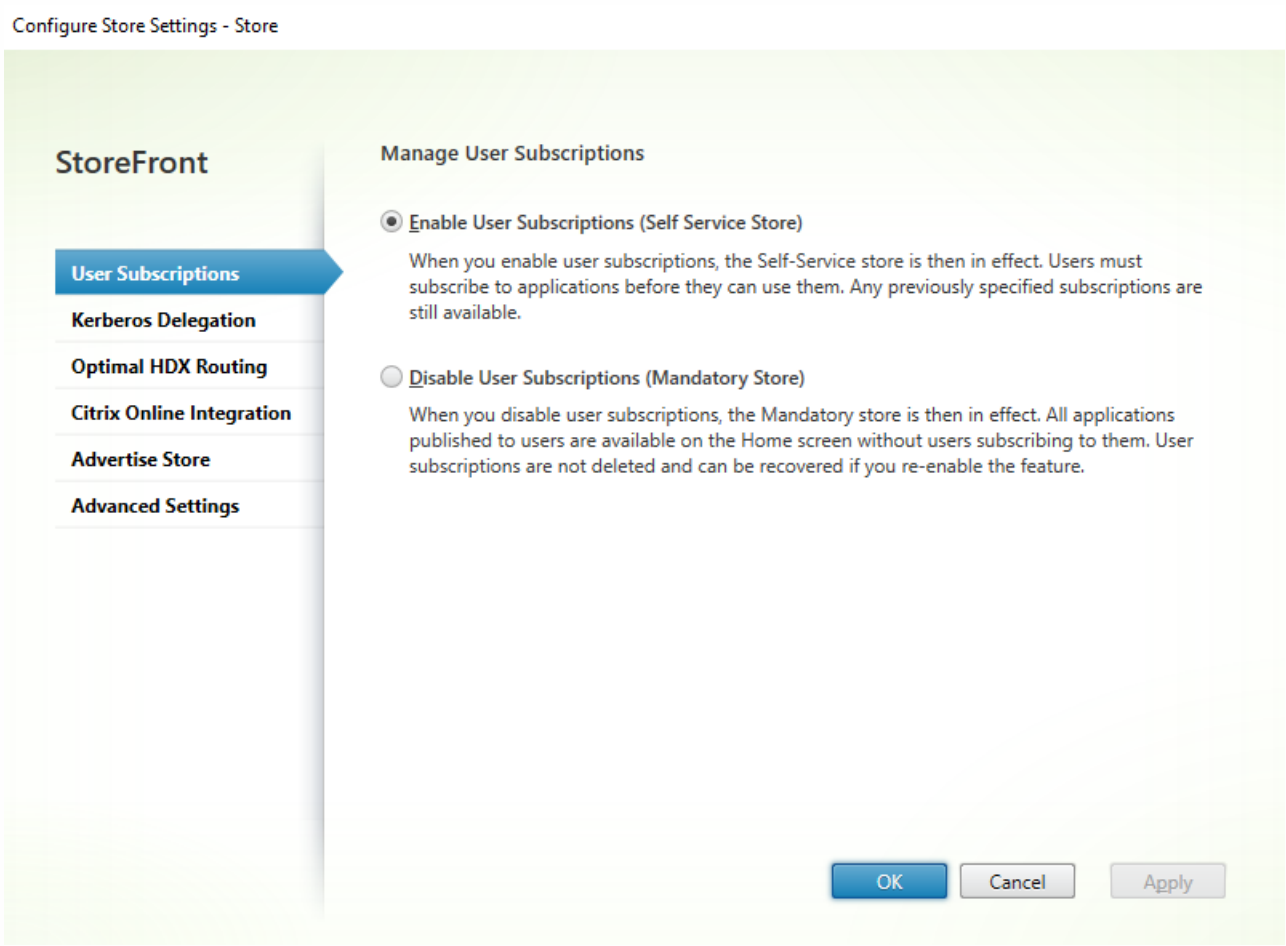
Configuración de las suscripciones de usuarios

Utilice la tarea "Suscripciones de usuarios" para seleccionar una de las siguientes opciones:

- Exigir que los usuarios se suscriban a las aplicaciones antes de usarlas (tienda de autoservicio).
- Permitir que los usuarios puedan recibir todas las aplicaciones cuando se conectan a la tienda (tienda obligatoria).

Inhabilitar las suscripciones de los usuarios a una tienda desde StoreFront también impide que se muestre la ficha Favoritos a los usuarios de Citrix Receiver. Inhabilitar las suscripciones no elimina los datos de suscripción a la tienda. Volver a habilitar las suscripciones a la tienda permitirá que un usuario vea las aplicaciones a las que está suscrito en Favoritos cada vez que inicie sesión.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel **Acciones**, haga clic en **Configurar parámetros de la tienda** > **Suscripciones de usuarios** para habilitar o inhabilitar la suscripción de usuarios.
3. Elija **Habilitar suscripciones de usuarios (tienda de autoservicio)** para que los usuarios tengan que suscribirse a las aplicaciones para utilizarlas. Las suscripciones previamente especificadas siguen estando disponibles.
4. Elija **Inhabilitar suscripciones de usuarios (tienda obligatoria)** para hacer que todas las aplicaciones publicadas estén disponibles para los usuarios en su página de inicio sin que tengan que suscribirse a ellas. Sus suscripciones no se eliminan y pueden recuperarlas si usted vuelve a habilitar la característica de suscripción.



En StoreFront 3.5 o versiones posteriores, puede utilizar el siguiente script de PowerShell para configurar las suscripciones de usuarios a una tienda:

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

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

Para obtener más información sobre Get-STFStoreService, consulte https://citrix.github.io/storefront-sdk/Citrix.StoreFront.Stores/Get-STFStoreService/

Administración de datos de suscripción a una tienda

Administre los datos de suscripción a una tienda mediante los cmdlets de PowerShell.

Nota

Use la consola de administración de StoreFront o PowerShell para administrar StoreFront. No use ambos métodos al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para cambiar la configuración de StoreFront. Citrix también recomienda que se realice una copia de seguridad de los datos de suscripción existente antes de realizar cambios, de modo que se pueda revertir a un estado anterior.

Purga de los datos de suscripción

Para cada tienda de la implementación, existe una carpeta y un almacén de datos de suscripción.

1. Detenga el servicio Citrix Subscriptions Store en el servidor StoreFront. Mientras el servicio Citrix Subscriptions Store esté en ejecución, no se puede eliminar datos de suscripción de cualquiera de las tiendas.
2. Busque la carpeta de suscripción de la tienda, ubicada en el servidor StoreFront: C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_
3. Elimine el contenido de la carpeta de suscripción de la tienda, pero no elimine la carpeta en sí.
4. Vuelva a iniciar el servicio Citrix Subscriptions Store en el servidor StoreFront.

En StoreFront 3.5 o versiones posteriores, puede utilizar el siguiente script de PowerShell para purgar los datos se suscripción a una tienda: Ejecute esta función PowerShell como un administrador con derechos para detener o iniciar servicios y eliminar archivos. Esta función PowerShell tiene el mismo resultado que los pasos manuales descritos anteriormente.

Para ejecutar los cmdlets de manera efectiva, el servicio Citrix Subscriptions Store debe estar ejecutándose en el servidor.

Code COPIAR

```
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"
```

Exportar datos de suscripción

Puede obtener una copia de seguridad de los datos de suscripción a la tienda en el formato de archivo TXT con texto separado por tabulaciones. Para ello, ejecute el siguiente cmdlet de PowerShell.

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

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

Si administra una implementación con varios servidores, puede ejecutar este cmdlet de PowerShell en cualquier servidor del grupo de servidores StoreFront. Cada servidor del grupo de servidores mantiene una copia sincronizada idéntica de los datos de suscripción proveniente de sus homólogos. Si cree que hay problemas con la sincronización de suscripciones entre los servidores StoreFront, exporte los datos de todos los servidores del grupo y compárelos para ver las diferencias.

Restauración de los datos de suscripción

Use Restore-STFStoreSubscriptions para sobrescribir los datos existentes de suscripción. Puede restaurar los datos de suscripción a una tienda con la ayuda de la copia de seguridad del archivo TXT que contiene texto separado con tabulaciones que ha creado antes mediante Export-STFStoreSubscriptions.

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

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

Para obtener más información sobre Restore-STFStoreSubscriptions, consulte https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Restore-STFStoreSubscriptions/#restore-stfstoresubscriptions

Restauración de datos en un único servidor StoreFront

En una implementación de un solo servidor, no es necesario que finalice el servicio Subscriptions Store. Tampoco es necesario eliminar los datos de suscripción existentes antes de restaurarlos.

Restauración de datos en un grupo de servidores StoreFront

Para restaurar los datos de suscripción a un grupo de servidores, debe seguir estos pasos.

Ejemplo: implementación de un grupo de tres servidores StoreFront.

StoreFrontA

StoreFrontB

StoreFrontC

1. Haga una copia de los datos existentes de suscripción que contiene cualquiera de los tres servidores.
2. Detenga el servicio Subscriptions Store en los servidores StoreFrontB y C. Esta acción impide que los servidores envíen o reciban datos de suscripción durante la actualización de StoreFrontA.
3. Purgue los datos de suscripción que contienen los servidores StoreFrontB y C. Esta acción impide que haya diferencias entre los datos de suscripción restaurados.
4. Restaure los datos en StoreFrontA con el cmdlet Restore-STFStoreSubscriptions. No es necesario detener el servicio Subscriptions Store ni eliminar los datos de suscripción presentes en StoreFrontA (se sobrescriben durante la operación de restauración).
5. Vuelva a iniciar el servicio Subscriptions Store en los servidores StoreFrontB y C. Los servidores ya pueden recibir una copia de los datos procedente de StoreFrontA.
6. Espere a que todos los servidores se sincronicen. El tiempo necesario depende de la cantidad de registros que existan en StoreFrontA. Si todos los servidores se encuentran en una red local, la sincronización suele producirse rápidamente. En cambio, la sincronización de suscripciones a través de una conexión WAN puede tardar más.
7. Exporte los datos de StoreFrontB y C para confirmar que se ha completado la sincronización o consulte los contadores de Store Subscription.

Importación de datos de suscripción

Use Import-STFStoreSubscriptions cuando no hay datos de suscripción para la tienda. Este cmdlet también permite que los datos de suscripción se transfieran de una tienda a otra, además de permitir que esos datos se importen a servidores StoreFront recién aprovisionados.

Code COPIAR

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


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

Para obtener más información sobre Import-STFStoreSubscriptions, consulte https://citrix.github.io/storefront-sdk/Citrix.StoreFront.SubscriptionsStore/Import-STFStoreSubscriptions/#import-stfstoresubscriptions

Información detallada del archivo de datos de suscripción

El archivo de datos de suscripción es un archivo de texto que contiene una línea por suscripción de usuario. Cada línea es una secuencia de valores separada por tabulaciones:

...

Definición de los valores:

- <*user-identifier*>. Obligatorio. Una secuencia de caracteres que identifica al usuario. Es el identificador de seguridad de Windows perteneciente al usuario.
- <*resource-id*>. Obligatorio. Una secuencia de caracteres que identifica los recursos suscritos.
- . Obligatorio. Una secuencia de caracteres que identifica de forma única la suscripción. Este valor no se utiliza (aunque debe haber un valor presente en el archivo de datos).
- <*subscription-status*>. Obligatorio. El estado de la suscripción: suscrito o no suscrito.
- <*property-name*> y <*property-value*>. Optativos. Una secuencia de cero o más pares de valores y . Estos representan propiedades asociadas a la suscripción por parte de un cliente StoreFront (normalmente un Citrix Receiver). Una propiedad del mismo nombre con varios valores, representada por varios pares de nombre y valor (por ejemplo, "... MyProp A MyProp B ..." representa la propiedad MyProp con valores A, B).

Ejemplo:

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

Tamaño de los datos de suscripción en el disco del servidor StoreFront

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

Tamaño de los archivos .txt de importación y exportación

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

Contadores de suscripción de tienda

Puede usar los contadores de los monitores de rendimiento Windows de Microsoft (Inicio > Ejecutar > perfmon) para ver, por ejemplo, la cantidad total de registros de suscripción existente en el servidor o la cantidad de registros que se sincroniza entre grupos de servidores StoreFront.

Cómo ver contadores de suscripción mediante PowerShell

Code COPIAR

```
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"
```

Configuraciones de tienda multisitio con alta disponibilidad

Aug 14, 2017

En este artículo:

Para las tiendas que combinan recursos de varias implementaciones, en especial implementaciones dispersas geográficamente, puede configurar el equilibrio de carga y la conmutación por error entre implementaciones, la asignación de usuarios a implementaciones e implementaciones específicas de recuperación ante desastres para proporcionar recursos de alta disponibilidad. Allí donde haya configurado diferentes dispositivos NetScaler Gateway para sus implementaciones, puede definir el dispositivo óptimo para el acceso de los usuarios a cada una de las implementaciones.

Desde StoreFront 3.5, la consola de administración de StoreFront ha dado respaldo a varios escenarios multisitio. Citrix recomienda usar la consola de administración cuando cumpla sus requisitos particulares.

Configuración de la combinación y asignación de usuarios

La consola de administración de StoreFront permite:

- **Asignar usuarios a implementaciones:** Según la pertenencia a grupos de Active Directory, se puede limitar qué usuarios tienen acceso a implementaciones específicas.
- **Agrupar las implementaciones:** Puede especificar qué implementaciones tienen recursos que desea agrupar. Los recursos coincidentes procedentes de implementaciones agrupadas se presentan al usuario como un único recurso con alta disponibilidad.
- **Asociar una zona con una implementación:** Cuando se accede con NetScaler Gateway en una configuración de equilibrio de carga global, StoreFront da prioridad a las implementaciones de las zonas que coincidan con la zona de la puerta de enlace al abrir recursos.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Compruebe que ha configurado la tienda con información de todas las implementaciones de XenDesktop y XenApp que quiera usar en la configuración. Para obtener más información sobre cómo agregar implementaciones a las tiendas, consulte Administración de los recursos disponibles en tiendas.
2. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
3. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Delivery Controllers**.
4. Si hay definidos dos o más Controllers, haga clic en **Configuración de la combinación multisitio y asignación de usuarios > Configurar**.
5. Haga clic en **Asignar usuarios a Controllers** y realice las selecciones necesarias en las pantallas para especificar los Delivery Controllers que se encuentran disponibles para cada usuario.
6. Haga clic en **Agrupar recursos**, seleccione los Controllers y haga clic **Agrupar** para especificar si los Delivery Controllers se agrupan. Si habilita la combinación de los Delivery Controllers, las aplicaciones y los escritorios de esos Delivery Controllers que tengan el mismo nombre y la misma ruta se presentarán como una sola aplicación o escritorio en Citrix Receiver.
7. Elija una o ambas casillas en los **Parámetros de Controllers agrupados** y haga clic en **Aceptar**.

   Los Controllers publican recursos idénticos: Cuando esta casilla está marcada, StoreFront enumera los recursos desde solo uno de los Controllers agregados. Cuando se deja sin marcar, StoreFront enumera los recursos de todos los Controllers en el conjunto agrupado (para acumular el conjunto entero de recursos disponibles del usuario). Al seleccionar esta opción se ofrece un mejor rendimiento para enumerar recursos, pero no se recomienda a menos que esté seguro de que la lista de recursos es idéntica en todas las implementaciones agrupadas.

   Equilibrar la carga de los recursos entre los Controllers: Cuando esta opción está marcada, los inicios de recursos se distribuyen de forma uniforme entre los Controllers disponibles. Si se deja sin marcar, los inicios de recursos se dirigen al primer Controller especificado en el diálogo de asignación de usuarios, y en caso de error, se pasa al siguiente Controller sucesivamente.

Configuraciones avanzadas

Aunque en la consola de administración de StoreFront se pueden configurar muchas operaciones comunes relacionadas con el funcionamiento multisitio y con alta disponibilidad, también puede configurar StoreFront usando los archivos de configuración de la misma manera que en las versiones anteriores de StoreFront.

Hay más funciones disponibles mediante PowerShell o mediante la edición de los archivos de configuración de StoreFront:

- La capacidad para especificar varias agrupaciones de implementaciones para agruparlas.
  - La consola de administración solo permite una sola agrupación de implementaciones, que es suficiente para la mayoría de los casos.
  - Para tiendas con implementaciones que tengan conjuntos de recursos dispares, se pueden conseguir mejoras aplicando agrupaciones múltiples.
- La capacidad para especificar un nivel de preferencia complejo para implementaciones agrupadas. La consola de administración permite equilibrar la carga de implementaciones agrupadas, o usarlos como una lista de servidores de conmutación por error.
- La capacidad para definir las implementaciones de recuperación ante desastres (implementaciones a las que solo se tiene acceso cuando las otras no estén disponibles).

Advertencia: Después de configurar las opciones avanzadas de sitios mediante la edición manual del archivo de configuración, algunas tareas dejan de estar disponibles en la consola de administración de Citrix StoreFront para evitar errores de configuración.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Compruebe que ha configurado la tienda con información de todas las implementaciones de XenDesktop y XenApp que quiera usar en la configuración, incluidas las implementaciones de recuperación ante desastres. Para obtener más información sobre cómo agregar implementaciones a las tiendas, consulte Administración de los recursos disponibles en tiendas.
2. Utilice un editor de texto para abrir el archivo web.config de la tienda, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storename\, donde storename es el nombre especificado para la tienda durante su creación.
3. Localice la siguiente sección en el archivo.

4. Especifique la configuración tal y como se muestra a continuación.

```
...

aggregationGroup="aggregationgroupname">

...

...

...

...
```

Utilice los siguientes elementos para definir la configuración.

- **userFarmMapping**

: Especifica los grupos de implementaciones y define el comportamiento del equilibrio de carga y la conmutación por error entre las implementaciones. Identifica las implementaciones que se van a usar para la recuperación ante desastres. Controla el acceso de los usuarios a los recursos mediante la asignación de grupos de usuarios de Microsoft Active Directory a los grupos de implementaciones especificados.

- **groups**
  Especifica los nombres y los identificadores de seguridad (SID) de los grupos de usuarios de Active Directory a los que se aplica la asignación asociada. Los nombres de los grupos de usuarios deben especificarse en el formato *dominio**grupo de usuarios*. Allí donde aparezca más de un grupo, la asignación se aplica solo a los usuarios que son miembros de todos los grupos especificados. Para habilitar el acceso para todas las cuentas de usuario de Active Directory, configure el nombre de grupo y SID con el valor **Everyone**.
- **equivalentFarmSet**
  : Especifica un grupo de implementaciones equivalentes que proporcionan recursos, para combinarlos con fines de equilibrio de carga o conmutación por error, además de un grupo asociado de implementaciones de recuperación ante desastres (optativo).

  El atributo **loadBalanceMode** determina la asignación de usuarios a implementaciones. Establezca el valor del atributo **loadBalanceMode** a **LoadBalanced** para asignar aleatoriamente usuarios a implementaciones en el conjunto de implementaciones equivalente, lo que distribuye de manera uniforme a los usuarios en todas las implementaciones. Cuando el valor del atributo **loadBalanceMode** está establecido en **Failover**, los usuarios se conectan a la primera implementación disponible en el orden en el que aparecen en la configuración, lo que reduce el número de implementaciones en uso en un momento dado. Especifique los nombres de los grupos de agregación para identificar los conjuntos de implementaciones equivalentes que proporcionan recursos para combinarse. Los recursos proporcionados por los conjuntos de implementaciones equivalentes que pertenecen al mismo grupo de agregación se combinan en uno. Para especificar que las implementaciones definidas en un determinado conjunto de implementaciones equivalente no deben combinarse con otras, establezca el nombre del grupo de agregación con una cadena vacía **""**.

  El atributo **identical** acepta los valores **True** y **False**, y especifica si todas las implementaciones dentro de un conjunto de implementaciones equivalentes proporcionan exactamente el mismo conjunto de recursos. Cuando las implementaciones son idénticas, StoreFront enumera los recursos de los usuarios desde una sola implementación principal del conjunto. Cuando las implementaciones proporcionan recursos que coinciden parcialmente pero no son idénticos, StoreFront enumera recursos desde cada una las implementaciones para obtener el conjunto completo de recursos disponibles para un usuario. El equilibrio de carga (en el momento de iniciar recursos) puede tener lugar independientemente de si las implementaciones son idénticas o no. El valor predeterminado para el atributo **identical** es false, aunque define como **true** cuando StoreFront se actualiza para evitar la modificación del comportamiento existente.

- **primaryFarmRefs**
  : Especifica un conjunto de sitios equivalentes de XenDesktop o XenApp donde coinciden todos o algunos de los recursos. Escriba los nombres de las implementaciones que ya se han agregado a la tienda. Los nombres de las implementaciones que especifique deben coincidir exactamente con los nombres que ha especificado al agregar las implementaciones a la tienda.
- **optimalGatewayForFarms**
  Especifica grupos de implementaciones y define los dispositivos NetScaler Gateway óptimos para que los usuarios accedan a los recursos proporcionados por estas implementaciones. Por lo general, el dispositivo óptimo para una implementación se coloca en la misma ubicación geográfica que la implementación. Solo debe definir los dispositivos NetScaler Gateway óptimos para implementaciones donde el dispositivo a través del cual los usuarios acceden a StoreFront no es el mejor.

Configuración de la sincronización de suscripciones

Para configurar una sincronización periódica de las suscripciones a aplicaciones de los usuarios entre tiendas de diferentes implementaciones de StoreFront, ejecute comandos de Windows PowerShell.

Nota: Las consolas de StoreFront y PowerShell no pueden estar abiertas al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.
Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.
Al establecer la sincronización de suscripciones, tenga en cuenta que los Delivery Controllers configurados deben tener nombres idénticos en las tiendas sincronizadas, y que los nombres distinguen entre mayúsculas y minúsculas. Si no duplica el nombre exacto de los Delivery Controllers se pueden crear suscripciones diferentes para los usuarios en las tiendas sincronizadas.

1. Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell y, en el símbolo del sistema, escriba los siguientes comandos para importar los módulos de StoreFront.
   Import-Module "installationlocation\Management\Cmdlets\UtilsModule.psm1" Import-Module "installationlocation\Management\Cmdlets\ SubscriptionSyncModule.psm1"
   Donde installationlocation es el directorio en el que StoreFront está instalado, normalmente C:\Archivos de programa\Citrix\Receiver StoreFront\.

2. Para especificar la implementación remota de StoreFront que contiene la tienda que se va a sincronizar, escriba el siguiente comando.
   Add-DSSubscriptionsRemoteSyncCluster -clusterName deploymentname -clusterAddress deploymentaddress
   Donde deploymentname es un nombre que le ayuda a identificar la implementación remota y deploymentaddress es la dirección del servidor StoreFront o grupo de servidores con equilibro de carga, accesibles desde el exterior, para la implementación remota.

3. Para especificar la tienda remota con la que se sincronizan las suscripciones a aplicaciones de los usuarios, escriba el siguiente comando.
   Add-DSSubscriptionsRemoteSyncStore -clusterName deploymentname -storeName storename
   Donde deploymentname es el nombre que ha definido para la implementación remota en el paso anterior y storename es el nombre especificado para las tiendas locales y remotas cuando se crearon. Para sincronizar suscripciones a aplicaciones entre las tiendas, las dos tiendas deben tener el mismo nombre en sus respectivas implementaciones de StoreFront.

4. Para configurar que la sincronización tenga lugar en determinados momentos del día, escriba el siguiente comando.
   Add-DSSubscriptionsSyncSchedule -scheduleName synchronizationname -startTime hh:mm
   Donde synchronizationname es un nombre que ayuda a identificar la programación que está creando. Use el parámetro -startTime para especificar la hora del día a la que quiere sincronizar las suscripciones entre las tiendas. Configure programaciones adicionales para especificar otras horas de sincronización durante el día.

5. De forma alternativa, para configurar una sincronización regular en un intervalo específico, escriba el siguiente comando.
   Add-DSSubscriptionsSyncReoccuringSchedule -scheduleName synchronizationname -startTime hh:mm:ss -repeatMinutes interval
   Donde synchronizationname es un nombre que ayuda a identificar la programación que está creando. Use el parámetro -startTime para especificar la hora del día a la que quiere comenzar la programación recurrente. Para interval, especifique el tiempo, en minutos, que debe transcurrir entre cada sincronización.

6. Agregue las cuentas de máquinas del dominio de Microsoft Active Directory para cada servidor StoreFront de la implementación remota al grupo de usuarios locales de Windows CitrixSubscriptionSyncUsers del servidor actual.
   Esto permite que los servidores de la implementación remota puedan acceder al servicio de almacenamiento de suscripciones en la implementación local una vez que ha configurado una programación de sincronización en la implementación remota. El grupo CitrixSubscriptionSyncUsers se crea automáticamente al importar el módulo de sincronización de suscripciones en el paso 1. Para obtener más información sobre cómo modificar grupos locales de usuarios, consulte http://technet.microsoft.com/es-es/library/cc772524.aspx.

7. Si su implementación local de StoreFront se compone de varios servidores, use la consola de administración de Citrix StoreFront para propagar los cambios de configuración a los demás servidores del grupo.
   Para obtener más información acerca de la propagación de cambios en una implementación con varios servidores StoreFront, consulte Configuración de grupos de servidores.

8. Repita los pasos 1 al 7 en la implementación remota de StoreFront para configurar una programación complementaria de sincronización de suscripciones de la implementación remota a la implementación local.
   Al configurar las programaciones de sincronización para sus implementaciones de StoreFront, asegúrese de que las programaciones no producen situaciones en las que las implementaciones intentan sincronizarse de forma simultánea.

9. Para iniciar la sincronización de las suscripciones a aplicaciones de los usuarios entre las tiendas, reinicie el servicio de almacenamiento de suscripciones en las implementaciones locales y remotas. En una línea de comandos de Windows PowerShell de un servidor de cada implementación, escriba el siguiente comando.
   Restart-DSSubscriptionsStoreSubscriptionService
10. Para quitar una programación de sincronización de suscripciones existente, escriba el siguiente comando. A continuación, propague el cambio de configuración por el resto de servidores StoreFront en la implementación y reinicie el servicio de almacenamiento de suscripciones.
    Remove-DSSubscriptionsSchedule -scheduleName synchronizationname
    Donde synchronizationname es el nombre que usted especificó para la programación al crearla.

11. Para ver una lista de las programaciones de sincronización de suscripciones actualmente configuradas para su implementación de StoreFront, escriba el siguiente comando.
    Get-DSSubscriptionsSyncScheduleSummary

Configuración del enrutamiento óptimo de HDX para una tienda

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

La diferencia entre una comunidad y una zona al definir asignaciones óptimas de puerta de enlace para una tienda

En las versiones de StoreFront anteriores a la versión 3.5, se podía asignar solo una puerta de enlace óptima solo a una comunidad o comunidades. El concepto de zona le permite dividir una implementación de XenApp 7.8 o XenDesktop 7.8 en varias zonas basándose en el centro de datos o la ubicación geográfica donde residen los Controllers de XenApp o XenDesktop y los recursos publicados. Defina las zonas en XenApp o XenDesktop 7.8 Studio. StoreFront ahora funciona conjuntamente con XenApp 7.8 y XenDesktop 7.8 y las zonas que se definan en StoreFront deben coincidir exactamente con los nombres de zona definidos en XenApp y XenDesktop.

Esta versión de StoreFront también permite crear una asignación de puerta de enlace óptima para todos los Delivery Controllers ubicados en la zona definida. La asignación de una zona a una puerta de enlace óptima es una operación casi idéntica a la creación de zonas usando comunidades de servidores, con lo que usted quizá esté más familiarizado. La única diferencia es que las zonas normalmente representan contenedores mucho más grandes, con muchos más Delivery Controllers. No es necesario agregar cada Delivery Controller a la asignación de una puerta de enlace óptima. Para colocar los Controllers en la zona deseada, solo tiene que etiquetar cada Delivery Controller con un nombre de zona que coincida con una zona ya definida en XenApp o XenDesktop. Se puede asignar una puerta de enlace óptima a más de una zona, pero normalmente se usa una sola zona. Una zona representa normalmente un centro de datos en una ubicación geográfica. Es de esperar que cada zona tenga como mínimo un NetScaler Gateway óptimo que se utiliza para conexiones HDX con los recursos de esa zona.

Para obtener más información acerca de este tema, consulte Zonas.

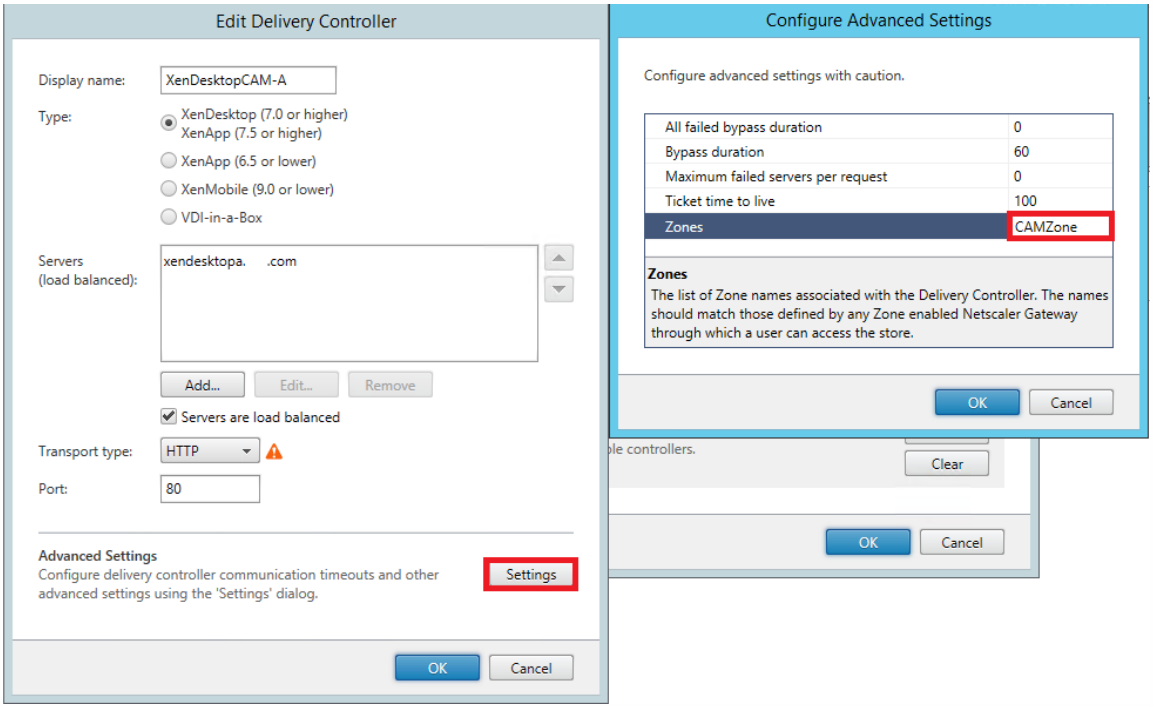
Cómo colocar un Delivery Controller en una zona

Defina el atributo de zona en cada Delivery Controller que quiere colocar dentro de una zona.

1. En la pantalla de **Inicio** o Aplicaciones de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Delivery**

Controllers.

3. Seleccione un Controller, haga clic en **Modificar**, y luego haga clic en **Parámetros** en la pantalla **Modificar Delivery Controller**.
4. En la fila **Zonas**, haga clic en la segunda columna.
5. Haga clic en **Agregar** en la pantalla **Nombres de zona de Delivery Controller** y agregue un nombre de zona.



Configure el enrutamiento óptimo de NetScaler Gateway para mejorar el control del enrutamiento de la conexión ICA desde el motor HDX a los recursos publicados, tales como VDA de XenDesktop o aplicaciones publicadas de XenApp o XenDesktop mediante StoreFront. Por lo general, la mejor puerta de enlace para un sitio está situada en la misma ubicación geográfica.

Solo necesita definir los dispositivos NetScaler Gateway óptimos para aquellas implementaciones donde el dispositivo a través del cual los usuarios acceden a StoreFront no es la mejor puerta de enlace. Si los inicios de recursos deben redirigirse a través de la puerta de enlace que los solicita, StoreFront hace esto automáticamente.

Ejemplo de uso con comunidades de servidores

1 x Puerta de enlace en Reino Unido –> 1 x StoreFront en Reino Unido	–> Aplicaciones y escritorios locales en Reino Unido –> Aplicaciones y escritorios en EEUU, solo en caso de que fallen los del Reino Unido
1 x Puerta de enlace en EEUU –> 1 x StoreFront en EEUU	–> Aplicaciones y escritorios locales en EEUU –>Aplicaciones y escritorios locales en Reino Unido, solo en caso de fallo de EEUU

Una puerta de enlace en el Reino Unido proporciona acceso remoto a recursos alojados en el Reino Unido, tales como aplicaciones y escritorios, mediante un StoreFront ubicado en Reino Unido.

La puerta de enlace del Reino Unido tiene definidos dos NetScaler Gateway, uno en Reino Unido y otro en EEUU, y tiene comunidades de servidores de Reino Unido y EEUU en su lista de Delivery Controllers. Los usuarios del Reino Unido acceden a los recursos remotos a través de la puerta de enlace, StoreFront y comunidades de servidores colocados en la misma ubicación. Si los recursos del Reino Unido dejan de estar disponibles, pueden conectar con recursos de EEUU como solución alternativa temporal.

Sin el enrutamiento óptimo de puertas de enlace, todos los inicios de recursos ICA pasarían a través de la puerta de enlace del Reino Unido que hizo la solicitud de inicio, independientemente de dónde estén ubicados geográficamente los recursos. De manera predeterminada, las puertas de enlace utilizadas para realizar la solicitud de inicios de recursos son identificadas de manera dinámica por StoreFront cuando se hace una solicitud. El enrutamiento óptimo de puertas de enlace anula este comportamiento y obliga a hacer las conexiones de EEUU a través de la puerta de enlace más próxima a las comunidades de EEUU que ofrecen los escritorios y aplicaciones.

Nota: Solo se puede asignar una única puerta de enlace óptima por sitio, para cada tienda de StoreFront.

Ejemplo de uso con zonas

1 x ZonaCAM -> 2 x StoreFronts en Reino Unido	-> Cambridge, Reino Unido: Aplicaciones y escritorios -> Fort Lauderdale, EEUU Costa Este: Aplicaciones y Escritorios -> Bangalore, India: Aplicaciones y Escritorios
1 x ZonaFTL -> 2 x StoreFronts en EEUU	-> Fort Lauderdale, EEUU Costa Este: Aplicaciones y Escritorios -> Cambridge, Reino Unido: Aplicaciones y escritorios -> Bangalore, India: Aplicaciones y Escritorios
1 x ZonaBGL -> 2 x StoreFronts en India	-> Bangalore, India: Aplicaciones y Escritorios -> Cambridge, Reino Unido: Aplicaciones y escritorios -> Fort Lauderdale, EEUU Costa Este: Aplicaciones y Escritorios

Figura 1. Enrutamiento subóptimo de puertas de enlace

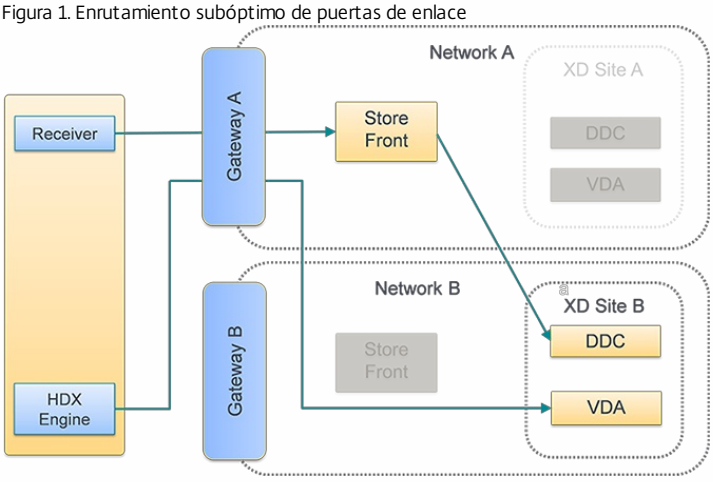
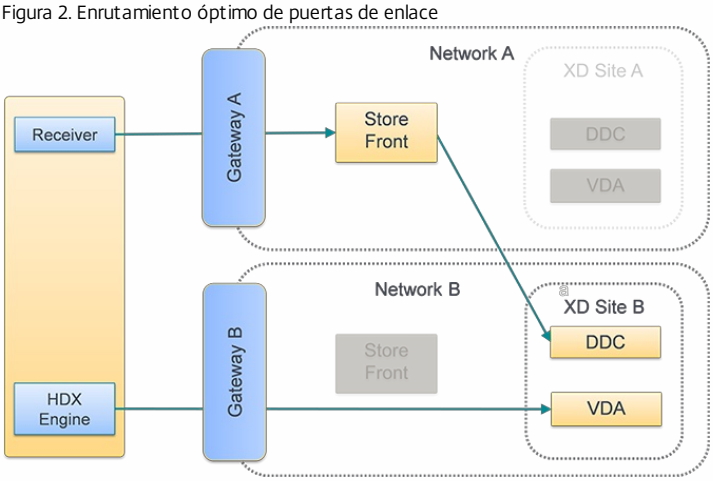


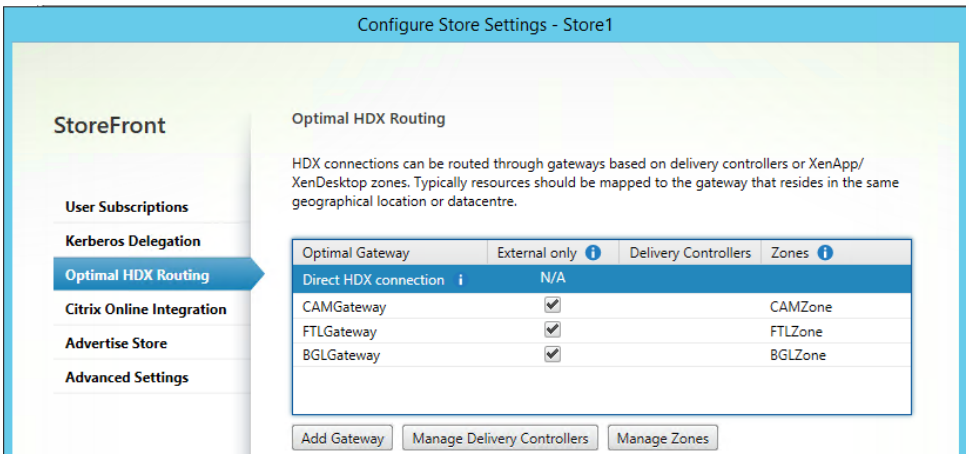
Figura 2. Enrutamiento óptimo de puertas de enlace



Use la consola de administración de Citrix StoreFront

Después de configurar diferentes dispositivos NetScaler Gateway para sus implementaciones, puede definir el dispositivo óptimo para el acceso de los usuarios a cada una de las implementaciones.

1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de **Citrix StoreFront** y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel **Acciones**, haga clic en **Configurar parámetros de la tienda**.
3. En la página **Parámetros** > **Enrutamiento óptimo de HDX**, seleccione una puerta de enlace.
4. Si marca la casilla **Solo externas**, esto es equivalente a usar **-enabledOnDirectAccess = false**, y la opción Conexión HDX directa es equivalente a usar **Set-DSFarmsWithNullOptimalGateway** para comunidades de servidores o zonas.



Agregar nueva puerta de enlace

Una de las opciones del procedimiento anterior es **Agregar puerta de enlace**. Después de elegir **Agregar puerta de enlace**, aparece la pantalla Agregar NetScaler Gateway.

1. En la pantalla **Parámetros generales**, complete los parámetros Nombre simplificado, URL de NetScaler Gateway y Uso o rol para configurar el acceso a las tiendas a través de NetScaler Gateway para los usuarios que se conectan desde redes públicas. El acceso remoto mediante NetScaler Gateway no se puede aplicar a tiendas no autenticadas.
2. En la pantalla **Secure Ticket Authority (STA)**, complete las opciones que se muestran. El STA está alojado en servidores XenDesktop y XenApp y emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.
3. En la pantalla **Parámetros de autenticación**, introduzca los parámetros que especifican cómo suministran sus credenciales los usuarios remotos.

Uso de PowerShell para configurar el enrutamiento óptimo de NetScaler Gateway para una tienda

Parámetros de API de PowerShell

Parameter	Description
-SiteId (entero)	ID del sitio dentro de IIS. Normalmente es 1 para el sitio en IIS donde StoreFront se instala de manera predeterminada.
-ResourcesVirtualPath	Ruta de la tienda que se va a configurar para tener una comunidad para la asignación de puerta de enlace óptima. Ejemplo: "/Citrix/Store"
-GatewayName	Nombre dado para identificar al NetScaler Gateway dentro de StoreFront. Ejemplo 1: ExternalGateway Ejemplo 2: InternalGateway
-Hostnames (matriz de cadenas)	Especifica el nombre de dominio completo (FQDN) y el puerto del dispositivo NetScaler Gateway óptimo. Example1 para el puerto estándar de vServer 443: gateway.example.com Example2 para el puerto no estándar de vServer 500: gateway.example.com:500
-Farms (matriz de cadenas)	Especifica un conjunto de implementaciones, normalmente colocadas en una misma ubicación, de XenDesktop, XenApp y App Controller que comparten el mismo dispositivo NetScaler Gateway óptimo. Una comunidad puede contener un solo Delivery Controller o varios Delivery Controllers que suministran los recursos publicados. Puede configurar un sitio de XenDesktop en StoreFront bajo Delivery Controllers como “XenDesktop”. Esto representa una única comunidad. Esto puede contener varios Delivery Controllers en su lista de conmutación por error: Ejemplo: "XenDesktop" XenDesktop-A.example.com XenDesktop-A.example.com XenDesktop-A.example.com
-Zones (matriz de cadenas)	Especifica un centro de datos o varios centros de datos que contienen muchos Delivery Controllers. Esto requiere etiquetar los objetos Delivery Controller de StoreFront con las zonas apropiadas a las que quiera asignarlos.
-staUrls (matriz de cadenas)	Especifica las direcciones URL de servidores XenDesktop o XenApp que ejecutan Secure Ticket Authority (STA). Si usa varias comunidades, incluya los servidores STA en cada una de ellas usando una lista de elementos separados por comas: Ejemplo: "http://xenapp-a.example.com/scripts/ctxsta.dll","http://xendesktop-a.example.com/scripts/ctxsta.dll"
-StasUseLoadBalancing (booleano)	Si tiene el valor True: obtiene aleatoriamente tiquets de sesión de todos los STA, distribuyendo de manera uniforme las solicitudes entre todos los STA. Si tiene el valor False: los usuarios se conectan al primer STA disponible en el orden en el que aparecen en la configuración, lo que reduce el número de STA que están en uso en un momento dado.
-StasBypassDuration	Establezca el tiempo en horas, minutos y segundos durante el que un STA se considera no disponible después de una solicitud fallida. Ejemplo: 02:00:00
-EnableSessionReliability (booleano)	Si tiene el valor True: mantiene abiertas las sesiones desconectadas mientras Receiver intenta reconectar automáticamente. Si ha configurado varios STA y desea asegurarse de que la fiabilidad de la sesión está siempre disponible, establezca el valor del atributo useTwoTickets en true para obtener tiquets de sesión de dos STA diferentes si un STA no está disponible durante la sesión.
-UseTwoTickets (booleano)	Si tienen el valor True: obtiene tiquets de sesión de dos STA diferentes para el caso de que uno de los STA deje de estar disponible durante la sesión. Si tiene el valor False: usa un único servidor STA.
-EnabledOnDirectAccess (booleano)	Si tiene el valor True: garantiza que cuando los usuarios locales de la red interna inician una sesión directamente en StoreFront, las conexiones con sus recursos se siguen enrutando a través del dispositivo óptimo definido para la comunidad. Si tiene el valor False: las conexiones a los recursos no se enrutan a través del dispositivo óptimo de la comunidad, a menos que los usuarios accedan a StoreFront mediante NetScaler Gateway.

Cuando los scripts de PowerShell abarcan varias líneas, como se muestra abajo, cada línea debe terminar con el carácter de comilla invertida.

Citrix recomienda copiar los ejemplos de código en el entorno ISE de PowerShell para validar el código de PowerShell con el validador de formato antes de ejecutarlo.

Configuración de una puerta de enlace óptima para una comunidad

> **Nota**
>
> La configuración del enrutamiento óptimo de HDX con el cmdlet antiguo de PowerShell llamado Set-DSOptimalGatewayForFarms no funciona.
>
> Como solución temporal para este problema:
>
> 1. Configure una puerta de enlace global con los parámetros que quiera para el enrutamiento óptimo de HDX. Para ello, use el comando Add-DSGlobalV10Gateway y suministre los valores predeterminados para los parámetros de autenticación.
> 2. Use el comando Add-DSStoreOptimalGateway para agregar la configuración de puerta de enlace óptima.
>
> Ejemplo:

```
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
```

Ejemplo:

Cree o sobrescriba las asignaciones de puerta de enlace óptima para comunidades en la tienda **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
```

Configuración de una puerta de enlace óptima para una zona

Ejemplo:

Cree o sobrescriba las asignaciones de puerta de enlace óptima para comunidades en la zona "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
```

Ejemplo:

Este script devuelve todas las asignaciones de puerta de enlace óptima para comunidades para la tienda llamada Internal.

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

Ejemplo:

Quitar todas las asignaciones de puerta de enlace óptima para las asignaciones de comunidades para la tienda llamada Internal.

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

Configurar conexiones HDX directas para comunidades

Ejemplo:

Este script impide que los inicios de ICA pasen a través de una puerta de enlace para la lista de comunidades especificadas para la tienda llamada Internal.

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/Store -Farms "Farm1","Farm2"
```

Ejemplo:

Este script devuelve todas las comunidades que están configuradas para impedir el paso de inicios de recursos ICA a través de una puerta de enlace para la tienda llamada Internal.

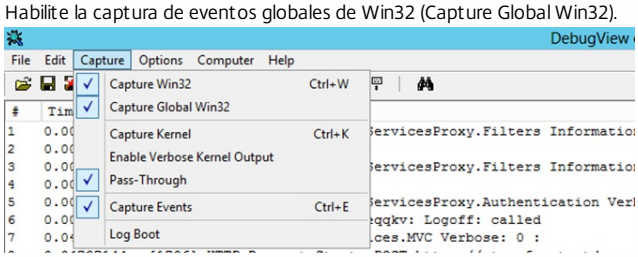
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/Internal"

Determine si StoreFront está usando las asignaciones de puerta de enlace óptima para comunidades

1. Habilite el seguimiento de StoreFront en todos los nodos del grupo de servidores usando PowerShell ejecutando:
   & "$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. Abra la herramienta de Vista de depuración en el escritorio de un servidor StoreFront. Si está usando un grupo de servidores StoreFront, puede que tenga que hacer esto en todos los nodos para asegurarse de que obtiene rastros de seguimiento del nodo que recibe la solicitud de inicio.
3. Habilite la captura de eventos globales de Win32 (Capture Global Win32).



4. Guarde los resultados del seguimiento en un archivo .log y abra dicho archivo en el Bloc de notas. Busque las entradas de registros que se muestran en los ejemplos a continuación.
5. Después, desactive el seguimiento, ya que esta función consume mucho espacio en el disco de los servidores StoreFront.
   Set-DSTraceLevel -All -TraceLevel Off

   Escenarios probados de puerta de enlace óptima

   - Un cliente externo inicia sesión en **Gateway1**. El inicio se redirige a través de la puerta de enlace óptima designada **Gateway2** para la comunidad **Farm2**.
     Set-DSOptimalGatewayForFarms -onDirectAccess=false

     Farm2 está configurada para usar la puerta de enlace óptima Gateway2.

     Farm2 tiene inhabilitado el uso de puerta de enlace óptima cuando el acceso es directo.

     Se usará la puerta de enlace óptima Gateway2 para el inicio.

   - Un cliente interno inicia sesión usando StoreFront. El inicio se redirige a través de la puerta de enlace óptima designada Gateway1 para la comunidad Farm1.
     Set-DSOptimalGatewayForFarms -onDirectAccess=true

     No se identifica dinámicamente ninguna puerta de enlace durante la solicitud. Se ha contactado con StoreFront de manera directa.

     Farm1 está configurada para usar la puerta de enlace óptima Gateway1.

     Farm1 tiene habilitado el uso de puerta de enlace óptima cuando el acceso es directo.

     Se usará la puerta de enlace óptima Gateway1 para lanzarla.

   - Un cliente interno inicia sesión usando Gateway1. Se impide el paso de inicios de recursos en Farm1 a través de cualquier puerta de enlace y se contacta con StoreFront directamente.
     Set-DSFarmsWithNullOptimalGateway

     Se identifica dinámicamente la puerta de enlace durante la solicitud: Gateway1

     Farm1 está configurada para no usar ninguna puerta de enlace. No se usará ninguna puerta de enlace para el inicio.

Integración con NetScaler Gateway y NetScaler

Aug 14, 2017

Puede utilizar NetScaler Gateway con StoreFront para ofrecer acceso remoto seguro a usuarios que se encuentren fuera de la red de la empresa. Asimismo, puede utilizar NetScaler para equilibrar la carga.

Planificación de uso de la puerta de enlace y el servidor de certificados

La integración de StoreFront con NetScaler y NetScaler Gateway requiere un plan para el uso del servidor de certificados y la puerta de enlace. Tenga en cuenta qué componentes de Citrix van a requerir certificados de servidor dentro de la implementación:

- Planifique la obtención de certificados para los servidores y puertas de enlace con conexión a Internet, de las entidades de certificación externas. Los dispositivos clientes podrían no confiar automáticamente en certificados de confianza firmados por una entidad interna.
- Planifique los nombres de servidor externos e internos. Muchas organizaciones tienen espacios de nombres independientes para cada caso, interno y externo - como ejemplo.com (externo) y ejemplo.net (interno). Un mismo certificado puede contener ambos tipos de nombre si se usa la extensión de nombre alternativo de sujeto (SAN). Esta práctica no se recomienda normalmente. Una entidad de certificación pública solo emitirá e un certificado si el dominio de nivel superior (Top Level Domain) está registrado en IANA. En este caso, algunos nombres de servidor internos comúnmente utilizados (por ejemplo, example.local) no se pueden usar, y se necesitarán certificados distintos para los nombres internos y externos de todos modos.
- Use certificados independientes para los servidores externos y los servidores internos, siempre que sea posible. Una puerta de enlace puede dar respaldo a varios certificados, mediante el vínculo de un certificado distinto a cada interfaz.
- Evite compartir certificados entre los servidores con conexión a Internet y los servidores sin conexión a Internet. Estos certificados serán probablemente diferentes, y tendrán distintos periodos de validez y distintas directivas de revocación que los certificados emitidos por entidades de certificación internas.
- Comparta certificados "comodín" solamente entre servicios que sean equivalentes. Evite compartir un certificado entre los diferentes tipos de servidor (por ejemplo, entre servidores StoreFront y otros tipos de servidores). Evite el uso compartido de un certificado entre los servidores que están bajo un control administrativo diferente, o que tengan directivas de seguridad diferentes. Algunos ejemplos típicos de servidores que proporcionan servicios equivalentes son:
  - Un grupo de servidores StoreFront y el servidor que ejecuta el equilibrio de carga entre ellos.
  - Un grupo de puertas de enlace con conexión a Internet dentro del equilibrio de carga global (GSLB).
  - Un grupo de Controllers de XenApp y XenDesktop 7.x, que proporcionan recursos equivalentes.
- Planifique el almacenamiento de claves privadas protegidas por hardware. Las puertas de enlace y los servidores, incluidos algunos modelos de NetScaler, pueden guardar la clave privada de forma segura dentro de un módulo de seguridad de hardware (HSM) o el módulo de plataforma segura (TPM). Por razones de seguridad, estas configuraciones normalmente no están diseñadas para compartir certificados y sus claves privadas. Consulte la documentación del componente. Si la implementa GSLB con NetScaler Gateway, esto puede requerir que cada puerta de enlace dentro del grupo de equilibrio de carga GSLB tenga un certificado idéntico, que contiene todos los nombres FQDN que desee usar.

Para obtener más información sobre cómo proteger la implementación de Citrix, consulte el documento técnico End-To-End Encryption with XenApp and XenDesktop y la sección Seguridad de XenApp y XenDesktop.

Cómo agregar una conexión de NetScaler Gateway

Aug 14, 2017

Utilice la tarea Agregar dispositivo NetScaler Gateway para agregar implementaciones de NetScaler Gateway a través de las cuales los usuarios pueden acceder a las tiendas. Debe habilitar el método de autenticación PassThrough desde NetScaler Gateway antes de poder configurar el acceso remoto a las tiendas a través de NetScaler Gateway. Para obtener más información acerca de la configuración de NetScaler Gateway para StoreFront, consulte Using WebFront to Integrate with StoreFront.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Administrar NetScaler Gateway.
3. Haga clic en **Agregar** y en la página Parámetros generales especifique un nombre para la implementación de NetScaler Gateway que ayude a los usuarios a identificarla.
   Los usuarios verán el nombre simplificado que especifique en Citrix Receiver, de modo que debe incluir la información relevante en el nombre para ayudarles a identificarlo y decidir si desean utilizar esa implementación o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de NetScaler Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.

4. Escriba la URL del servidor virtual o punto de entrada de usuarios (para Access Gateway 5.0) para la implementación. Especifique la versión de producto utilizada en la implementación.
   El nombre de dominio completo (FQDN) para la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de NetScaler Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de NetScaler Gateway.

5. Si va a agregar una implementación de Access Gateway 5.0, continúe en el paso 7. De lo contrario, especifique la dirección IP de subred del dispositivo NetScaler Gateway, si es necesario. Se necesita una dirección IP de subred para los dispositivos Access Gateway 9.3. Esta dirección es optativa si se trata de versiones más recientes de producto.
   La dirección de subred es la dirección IP que NetScaler Gateway utiliza para representar el dispositivo de usuario cuando se comunica con los servidores de la red interna. También puede ser la dirección IP asignada del dispositivo NetScaler Gateway. Cuando está especificada, StoreFront utiliza la dirección IP de subred para verificar que las solicitudes entrantes provienen de un dispositivo de confianza.

6. Si desea agregar un dispositivo con NetScaler Gateway 10.1-11.0, Access Gateway 10-11.0 o Access Gateway 9.3, seleccione en la lista Tipo de inicio de sesión el método de autenticación configurado en el dispositivo para los usuarios de Citrix Receiver.
   La información que proporcione sobre la configuración de su dispositivo NetScaler Gateway se agrega al archivo de aprovisionamiento para la tienda. Esto permite que Citrix Receiver envíe la solicitud de conexión pertinente al comunicarse con el dispositivo por primera vez.

   - Si es necesario que los usuarios introduzcan sus credenciales de dominio de Microsoft Active Directory, seleccione Dominio.
   - Si es necesario que los usuarios introduzcan un código de token obtenido de un token de seguridad, seleccione Token

de seguridad.
- Si es necesario que los usuarios introduzcan sus credenciales de dominio y un código de token obtenido de un token de seguridad, seleccione Dominio y token de seguridad.
- Si es necesario que los usuarios introduzcan una contraseña de un solo uso enviada por mensaje de texto, seleccione Autenticación SMS.
- Si es necesario que los usuarios presenten una tarjeta inteligente e introduzcan un PIN, seleccione Tarjeta inteligente.

Si configura la autenticación con tarjeta inteligente con un método secundario de autenticación (al que los usuarios puedan recurrir en caso de tener problemas con su tarjeta inteligente), seleccione el método secundario de autenticación en la lista Alternativa a tarjeta inteligente. Continúe en el paso 8.

7. Para agregar una implementación de Access Gateway 5.0, indique si el punto de entrada del usuario está alojado en un dispositivo independiente o en un servidor de Access Controller que forma parte de un clúster. Si desea agregar un clúster, haga clic en Siguiente y continúe en el paso 9.
8. Si desea configurar StoreFront para NetScaler Gateway 10.1-11.0, Access Gateway 10-11.0, Access Gateway 9.3 o un único dispositivo Access Gateway 5.0, complete la URL del servicio de autenticación de NetScaler Gateway en el cuadro URL de respuesta. StoreFront anexa automáticamente la parte estándar de la dirección URL. Haga clic en Siguiente y continúe en el paso 11.
   Escriba la URL internamente accesible del dispositivo. StoreFront se comunica con el servicio de autenticación de NetScaler Gateway para verificar que las solicitudes recibidas de NetScaler Gateway provienen de ese dispositivo.
9. Para configurar StoreFront para un clúster de Access Gateway 5.0, enumere en la página Dispositivos las direcciones IP o FQDN de los dispositivos del clúster y haga clic en Siguiente.
10. En la página Habilitar autenticación silenciosa, enumere las direcciones URL para el servicio autenticación que se ejecuta en los servidores de Access Controller. Agregue direcciones URL de varios servidores para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Haga clic en Siguiente.
    StoreFront utiliza el servicio de autenticación para realizar la autenticación de los usuarios remotos para que no necesiten volver a introducir sus credenciales cuando accedan a las tiendas.
11. En todas las implementaciones, para que los recursos proporcionados por XenDesktop o XenApp estén disponibles en la tienda, enumere en la página Secure Ticket Authority (STA) las direcciones URL de los servidores que ejecutan STA. Introduzca direcciones URL vinculadas a varios STA para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error.
    El STA está alojado en servidores XenDesktop y XenApp. Emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.
12. Si desea que XenDesktop y XenApp mantengan abiertas las sesiones desconectadas mientras Citrix Receiver intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y desea asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tiquets de dos STA, si están disponibles.
    Cuando la casilla Solicitar tiquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tiquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA no está disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.
13. Haga clic en Crear para agregar la información de la implementación de NetScaler Gateway. Una vez que la implementación se ha agregado, haga clic en Finalizar.

Para obtener más información sobre la actualización de la información de las implementaciones, consulte Configuración de los parámetros de conexión de NetScaler Gateway.

Para proporcionar acceso a las tiendas a través de NetScaler Gateway, se necesita una baliza interna y al menos dos balizas externas. Citrix Receiver utiliza balizas para determinar si los usuarios están conectados a redes locales o públicas y, luego, selecciona el método de acceso adecuado. De forma predeterminada, StoreFront utiliza la dirección URL del servidor o la dirección URL con equilibrio de carga de la implementación como baliza interna. El sitio Web de Citrix y la URL del servidor virtual o punto de entrada (para Access Gateway 5.0) de la primera implementación de NetScaler Gateway que usted agrega se utilizan como balizas externas de forma predeterminada. Para obtener más información sobre cómo cambiar balizas, consulte Configuración de balizas.

Para permitir que los usuarios accedan a los almacenes a través de NetScaler Gateway, compruebe que ha configurado el acceso de usuarios remotos para dichos almacenes.

Importación de un NetScaler Gateway

Aug 14, 2017

Los parámetros de acceso remoto configurados en la consola de administración de NetScaler deben ser idénticos a aquellos configurados en StoreFront. Este artículo muestra cómo importar un dispositivo NetScaler Gateway para que NetScaler y StoreFront están configurados correctamente para funcionar juntos.

Requisitos

- Se necesita NetScaler 11.1.51.21, o una versión posterior, para exportar varios servidores vServer de puerta de enlace a un archivo ZIP. **Nota**: NetScaler solo puede exportar los servidores virtuales de puerta de enlace que se creen mediante el asistente de XenApp y XenDesktop.
- DNS debe ser capaz de resolver todas las URL de los servidores STA (Secure Ticket Authority), y StoreFront debe ser capaz de contactar con ellos. Estas direcciones figuran en el archivo GatewayConfig.json en el archivo ZIP generado por NetScaler.
- El archivo GatewayConfig.json dentro del archivo ZIP generado por NetScaler debe contener la dirección URL de un sitio de Citrix Receiver para Web existente en el servidor StoreFront. NetScaler 11.1 (y versiones posteriores) se ocupa de esto poniéndose en contacto con el servidor StoreFront y enumerando todas las tiendas y sitios de Citrix Receiver para Web existentes, antes de generar el archivo ZIP para exportarlo.
- StoreFront debe ser capaz de resolver la URL de respuesta en DNS con la dirección IP del servidor virtual VPN de la puerta de enlace para la autenticación mediante la puerta de enlace importada.

    La combinación de URL de respuesta y puerto que use es normalmente la misma que la combinación de URL y puerto de la puerta de enlace, siempre que StoreFront pueda resolver esta URL.

    o

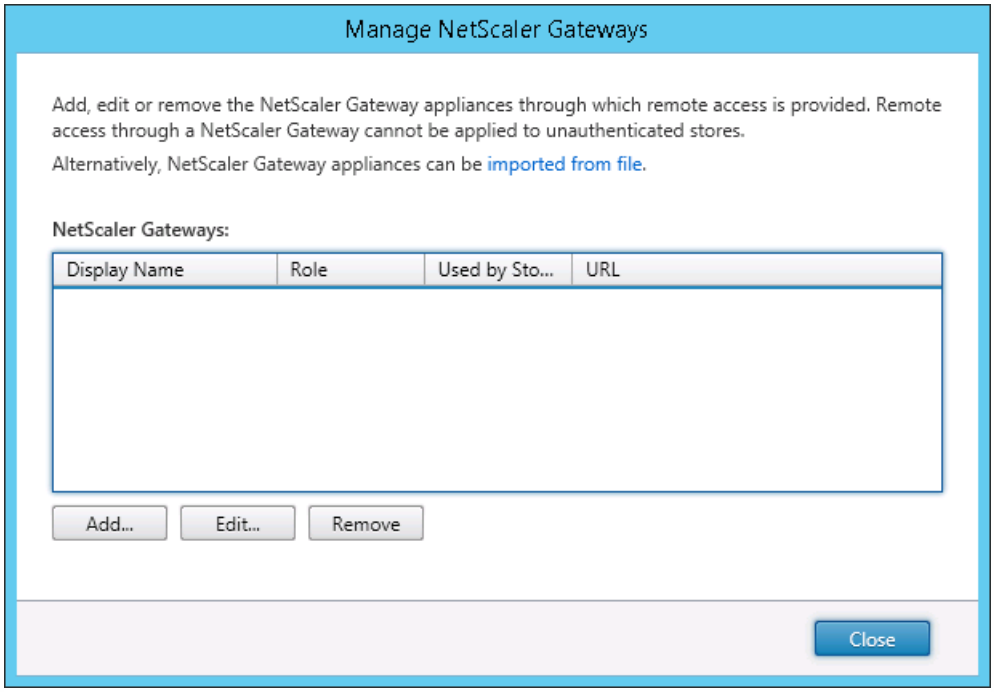
    La combinación de URL de respuesta y puerto puede ser diferente de la URL y puerto de la puerta de enlace, si usa nombres de espacios DNS distintos para uso externo e interno en su entorno. Si su puerta de enlace se encuentra en una zona desmilitarizada (DMZ) y usa una URL , y StoreFront se encuentra en la red privada de la empresa y usa una URL puede utilizar una URL de respuesta para apuntarla de vuelta al servidor virtual de la puerta de enlace en la DMZ.

Importar un NetScaler Gateway mediante la consola

Puede importar uno o varios dispositivos NetScaler Gateway mediante la importación de un archivo de configuración de NetScaler.

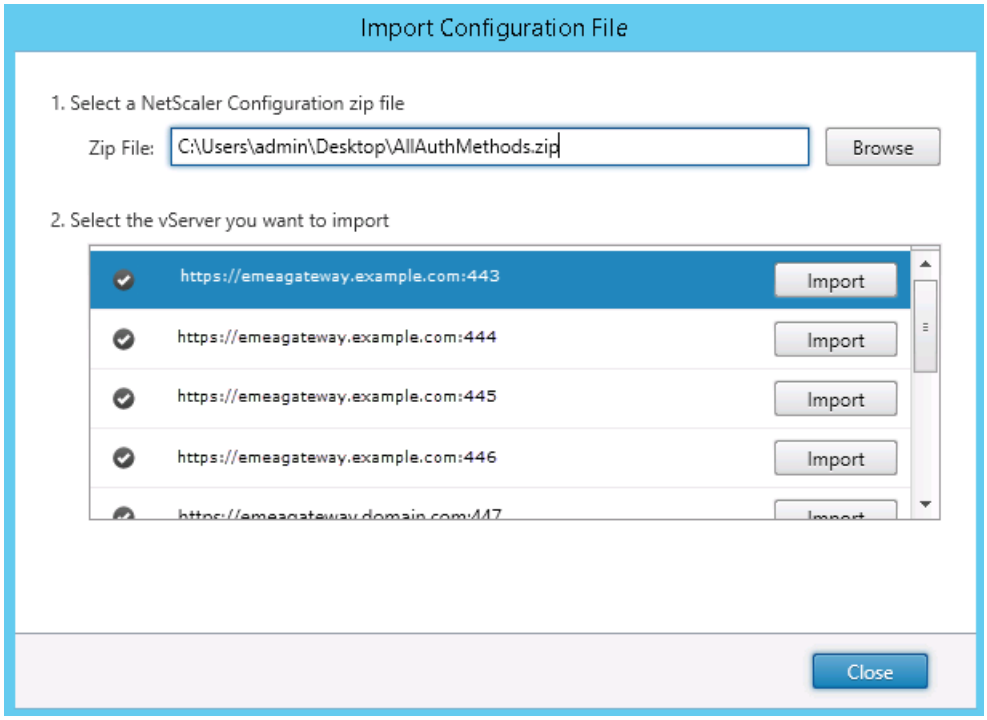
> ### Important
>
> Citrix no admite la edición manual del archivo de configuración exportado desde NetScaler.

1. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones,** haga clic en **Administrar NetScaler Gateway**.
2. En la pantalla Administrar NetScaler Gateway, haga clic en el enlace **Importar desde un archivo**.



3. Busque el archivo zip de configuración de NetScaler.

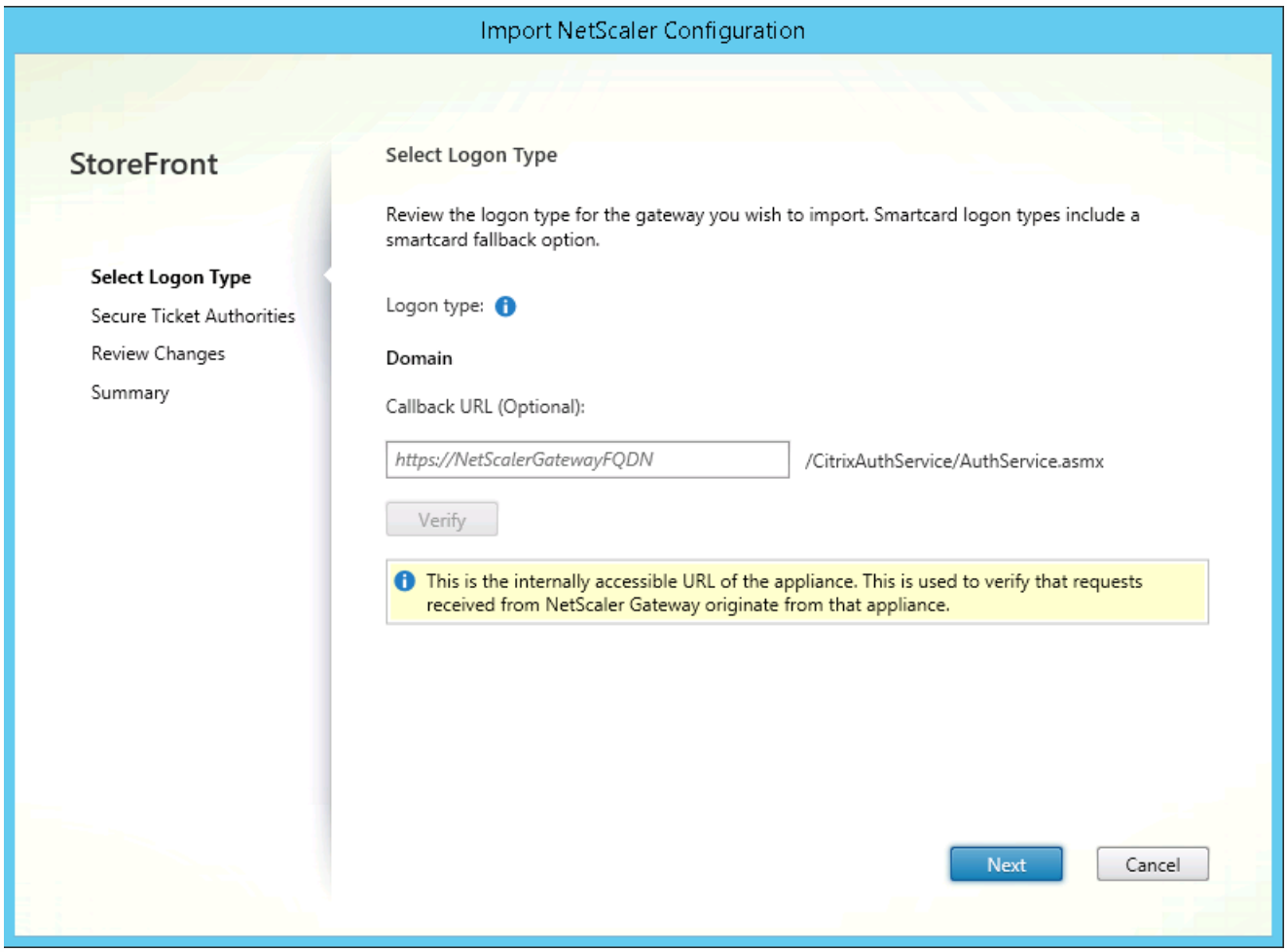
4. Se muestra una lista de servidores virtuales de puerta de enlace del archivo ZIP seleccionado. Seleccione el servidor virtual de puerta de enlace que desea importar y haga clic en **Importar**. Si se repite la importación de un servidor virtual, el botón Importar aparece como botón Actualizar. Si elige **Actualizar**, tendrá la opción más tarde para sobrescribir o crear una nueva puerta de enlace.



5. Revise el tipo de inicio de sesión para la puerta de enlace seleccionada y especifique una URL de respuesta si es necesario. El tipo de inicio de sesión es el método de autenticación configurado en el dispositivo NetScaler Gateway para los usuarios

de Citrix Receiver. Algunos tipos de inicio de sesión necesitan direcciones URL de respuesta (consulte la tabla).

- Haga clic en **Verificar** para comprobar si la URL de respuesta es válida y accesible desde el servidor StoreFront.



Tipo de inicio de sesión en la consola	**LogonType en el archivo JSON**	**URL de respuesta (requerida)**
Dominio	Dominio	NO
Dominio y token de seguridad	DomainAndRSA	NO
Token de seguridad	RSA	Sí
Tarjeta inteligente - Sin alternativa	SmartCard	Sí
Tarjeta inteligente - Dominio	SmartCardDomain	Sí
Tarjeta inteligente - Dominio y token	SmartCardDomainAndRSA	Sí

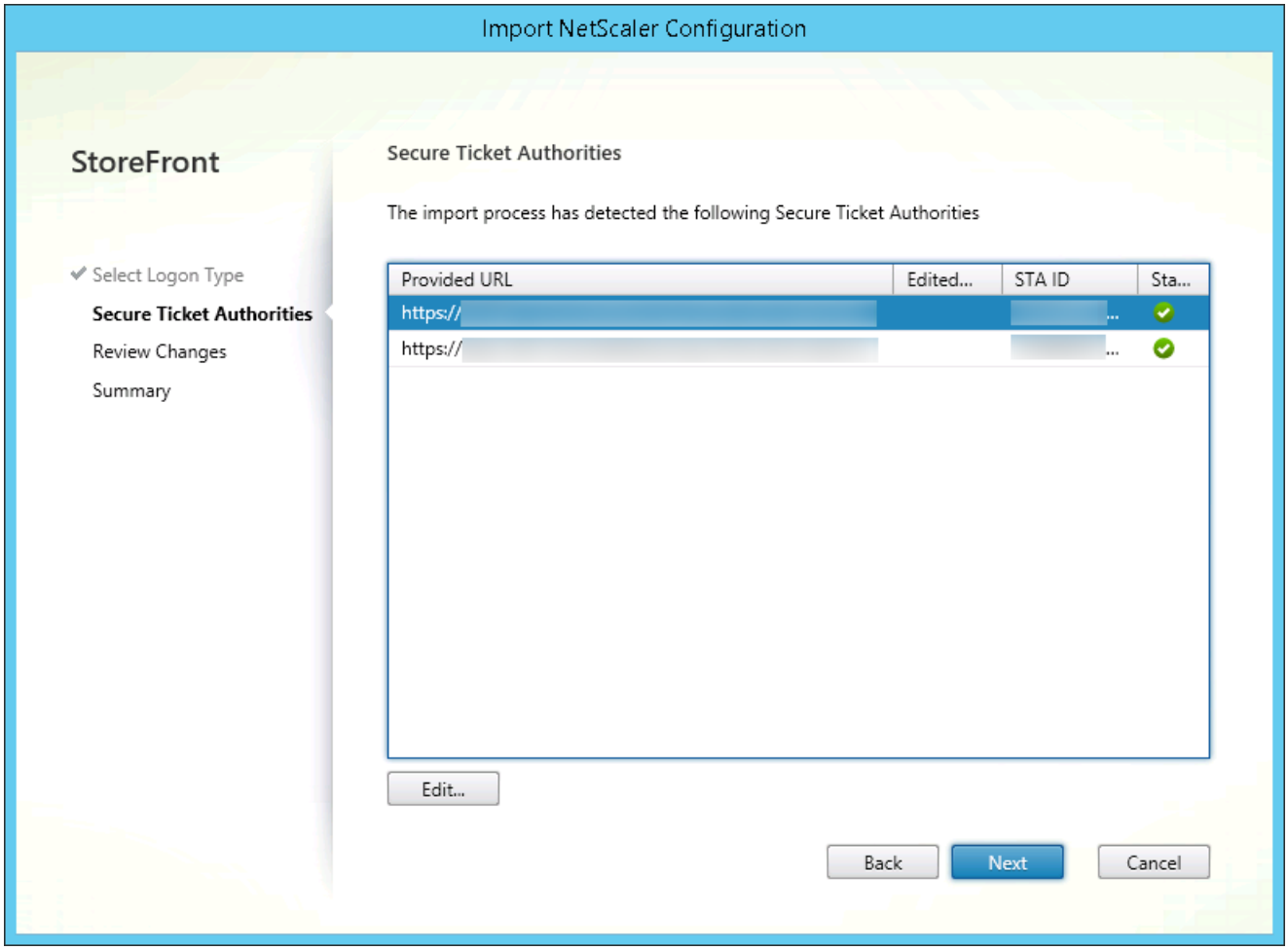
de seguridad		
Tarjeta inteligente - Token de seguridad	SmartCardRSA	Sí
Tarjeta inteligente - Autenticación SMS	SmartCardSMS	Sí
Autenticación SMS	SMS	Sí

Si se requiere una URL de respuesta, StoreFront rellenará la URL de respuesta en función de la URL de la puerta de enlace encontrada en el archivo ZIP. Se puede cambiar a cualquier dirección URL válida que haga referencia a la dirección IP del servidor virtual de NetScaler Gateway.

Si desea utilizar Smart Access, se necesita una URL de respuesta.

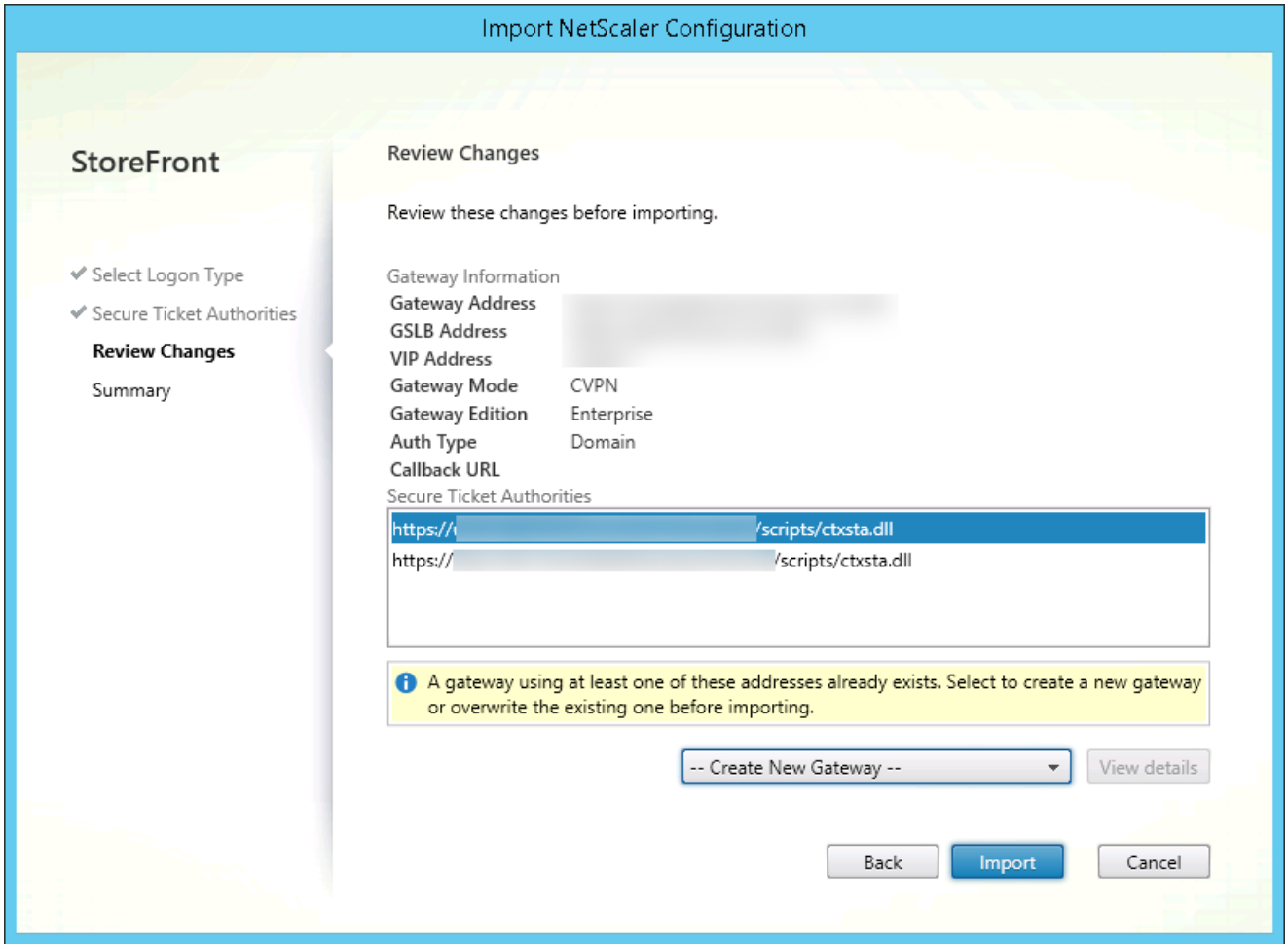
6. Haga clic en **Next**.

7. StoreFront contacta con todas las direcciones URL de servidor STA (Secure Ticket Authority) que figuran en el archivo ZIP que utilizan DNS y valida que sean servidores de generación de tiquets STA operativos. La importación no continuará si alguna o varias de las direcciones URL de STA no son válidas.



8. Haga clic en **Next**.

9 Revise los detalles de la importación. Si ya existe una puerta de enlace con la misma combinación de dirección URL y puerto (puerta de enlace:puerto), use la lista desplegable para seleccionar una puerta de enlace para sobrescribirla, o cree una nueva.



StoreFront utiliza la combinación de URL_PuertaDeEnlace:puerto para determinar si una puerta de enlace que se quiere importar coincide con otra ya existente que quiera actualizar. Si una puerta de enlace tiene una combinación URL_PuertaDeEnlace:puerto diferente, StoreFront la trata como si fuera una puerta de enlace nueva. Esta tabla de parámetros de puerta de enlace muestra los parámetros que se puede actualizar.

Parámetro de la puerta de enlace	**Puede actualizarse**
Combinación de URL de puerta de enlace URL:puerto	NO
URL de GSLB	Sí
Huella digital y certificado de confianza de NetScaler	Sí
URL de respuesta	Sí
URL del sitio de Citrix Receiver para Web	Sí
VIP/dirección de la puerta de enlace	Sí

ID de STA y URL de STA	Sí
Todos los tipos de inicio de sesión	Sí

10.Haga clic en **Importar**. Si el servidor StoreFront forma parte de un grupo de servidores, se muestra un mensaje donde se recuerda al usuario que tiene que propagar los parámetros de la puerta de enlace importada a los demás servidores del grupo.

11. Haga clic en **Finalizar**.

Para importar otra configuración de servidor virtual, repita los pasos anteriores.

> ## Nota
>
> La puerta de enlace predeterminada de una tienda es la puerta de enlace a través de la que los Citrix Receiver nativos intentan conectarse a menos que estén configurados para usar una puerta de enlace diferente. Si no hay ninguna puerta de enlace configurada para la tienda, la primera puerta de enlace que se importe desde el archivo ZIP se convertirá en la puerta de enlace predeterminada utilizada por los Citrix Receiver nativos. La importación de puertas de enlace subsiguientes no cambia la puerta de enlace predeterminada que se haya configurado ya para la tienda.

Importar varios NetScaler Gateway mediante PowerShell

Read-STFNetScalerConfiguration

- Copie el archivo ZIP en el escritorio del administrador de StoreFront conectado en ese momento.
- Lea el paquete ZIP importado de NetScaler ZIP en memoria y consulte las tres puertas de enlace que contiene usando sus valores de índice.

comando COPIAR

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Vea los tres objetos de puerta de enlace en memoria que se leyeron desde el paquete de importación ZIP de Netscaler con el cmdlet STFNetScalerConfiguration.

comando COPIAR

```
$ImportedGateways.Document.Gateways[0]

$ImportedGateways.Document.Gateways[1]
```

```
$ImportedGateways.Document.Gateways[2]



GatewayMode            : CVPN

CallbackUrl            :

GslbAddressUri         : https://gslb.example.com/

AddressUri             : https://emeagateway.example.com/

Address                : https://emeagateway.example.com:443

GslbAddress            : https://gslb.example.com:443

VipAddress             : 10.0.0.1

Stas                   : {STA298854503, STA909374257}

StaLoadBalance         : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType        : Domain

GatewayEdition         : Enterprise

ReceiverForWebSites    : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}



GatewayMode            : CVPN

CallbackUrl            :

GslbAddressUri         : https://gslb.example.com/

AddressUri             : https://emeagateway.example.com/
```



```
Address              : https://emeagateway.example.com:444
GslbAddress          : https://gslb.example.com:443
VipAddress           : 10.0.0.2
Stas                 : {STA298854503, STA909374257}
StaLoadBalance       : True
CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}
GatewayAuthType      : DomainAndRSA
GatewayEdition       : Enterprise
ReceiverForWebSites  : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}

GatewayMode          : CVPN
CallbackUrl          : https://emeagateway.example.com:445
GslbAddressUri       : https://gslb.example.com/
AddressUri           : https://emeagateway.example.com/
Address              : https://emeagateway.example.com:445
GslbAddress          : https://gslb.example.com:443
VipAddress           : 10.0.0.2
Stas                 : {STA298854503, STA909374257}
StaLoadBalance       : True
CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}
```

```
GatewayAuthType        :SmartCard

GatewayEdition         : Enterprise

ReceiverForWebSites    : {Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite}
```

Import-STFNetScalerConfiguration, sin especificar una URL de respuesta

Copie el archivo ZIP en el escritorio del administrador de StoreFront conectado en ese momento. Lea el paquete ZIP importado de NetScaler ZIP en memoria y consulte las tres puertas de enlace que contiene usando sus valores de índice.

comando COPIAR

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"
```

Importe tres puertas de enlace nuevas en StoreFront mediante el cmdlet Import-STFNetScalerConfiguration y especifique los índices de puerta de enlace que necesite. El parámetro -Confirm:$False evita que la interfaz de usuario de PowerShell le pregunte si quiere permitir importar cada una de las puertas de enlace. Quite este parámetro si quiere importar una por una las puertas de enlace.

comando COPIAR

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -Confirm:$False
```

Import-STFNetScalerConfiguration especificando su propia URL de respuesta

Importe tres nuevas puertas de enlace en StoreFront usando el cmdlet Import-STFNetScalerConfiguration y especifique la URL de respuesta que quiera usando el parámetro -callbackURL.

comando COPIAR

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.c

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.c

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.c
```

Import-STFNetScalerConfiguration, para anular el método de autenticación almacenado en el archivo de importación y permite especificar su propia URL de respuesta

- Importe tres nuevas puertas de enlace en StoreFront usando el cmdlet Import-STFNetScalerConfiguration y especifique la URL de respuesta que quiera usando el parámetro -callbackURL.

comando COPIAR

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://e

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://e

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://e
```

Configuración de los parámetros de conexión de NetScaler Gateway

Aug 14, 2017

Las siguientes tareas permiten actualizar la información de las implementaciones de NetScaler Gateway a través de las cuales los usuarios acceden a sus tiendas. Para obtener más información acerca de la configuración de NetScaler Gateway para StoreFront, consulte Using WebFront to Integrate with StoreFront.

Si realiza cambios en sus implementaciones de NetScaler Gateway, asegúrese de que los usuarios que acceden a las tiendas a través de estas implementaciones actualicen Citrix Receiver con la información de conexión modificada. Cuando un sitio de Citrix Receiver para Web está configurado para una tienda, los usuarios pueden obtener un archivo de aprovisionamiento de Citrix Receiver actualizado desde el sitio. De lo contrario, puede exportar un archivo de aprovisionamiento para la tienda y poner este archivo a disposición de los usuarios.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Cambios en la configuración general de NetScaler Gateway

Utilice la tarea Cambiar parámetros generales para modificar los nombres de las implementaciones de NetScaler Gateway que se muestran a los usuarios, actualizar StoreFront con los cambios en el servidor virtual o la URL del punto de entrada de usuarios, y el modo de implementación de la infraestructura de NetScaler Gateway.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Administrar NetScaler Gateway.
3. Especifique un nombre para la implementación de NetScaler Gateway que ayude a los usuarios a identificarla.
   Los usuarios verán el nombre simplificado que especifique en Citrix Receiver, de modo que debe incluir la información relevante en el nombre para ayudarles a identificarlo y decidir si desean utilizar esa implementación o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de NetScaler Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.
4. Escriba la URL del servidor virtual o punto de entrada de usuarios (para Access Gateway 5.0) para la implementación. Especifique la versión de producto utilizada en la implementación.
   El nombre de dominio completo (FQDN) para la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de NetScaler Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de NetScaler Gateway.
5. Si la implementación está ejecutando Access Gateway 5.0, continúe en el paso 7. De lo contrario, especifique la dirección IP de subred del dispositivo NetScaler Gateway, si es necesario. Se necesita una dirección IP de subred para los dispositivos Access Gateway 9.3. Esta dirección es optativa si se trata de versiones más recientes de producto.
   La dirección de subred es la dirección IP que NetScaler Gateway utiliza para representar el dispositivo de usuario cuando se comunica con los servidores de la red interna. También puede ser la dirección IP asignada del dispositivo NetScaler Gateway. Cuando está especificada, StoreFront utiliza la dirección IP de subred para verificar que las solicitudes entrantes provienen de un dispositivo de confianza.

6. Si su dispositivo está ejecutando NetScaler Gateway 10.1-11.0, Access Gateway 10-11.0 o Access Gateway 9.3, seleccione en la lista Tipo de inicio de sesión el método de autenticación configurado en el dispositivo para los usuarios de Citrix Receiver.
   La información que proporcione sobre la configuración de su dispositivo NetScaler Gateway se agrega al archivo de aprovisionamiento para la tienda. Esto permite que Citrix Receiver envíe la solicitud de conexión pertinente al comunicarse con el dispositivo por primera vez.

   - Si es necesario que los usuarios introduzcan sus credenciales de dominio de Microsoft Active Directory, seleccione Dominio.
   - Si es necesario que los usuarios introduzcan un código de token obtenido de un token de seguridad, seleccione Token de seguridad.
   - Si es necesario que los usuarios introduzcan sus credenciales de dominio y un código de token obtenido de un token de seguridad, seleccione Dominio y token de seguridad.
   - Si es necesario que los usuarios introduzcan una contraseña de un solo uso enviada por mensaje de texto, seleccione Autenticación SMS.
   - Si es necesario que los usuarios presenten una tarjeta inteligente e introduzcan un PIN, seleccione Tarjeta inteligente.

   Si configura la autenticación con tarjeta inteligente con un método secundario de autenticación (al que los usuarios puedan recurrir en caso de tener problemas con su tarjeta inteligente), seleccione el método secundario de autenticación en la lista Alternativa a tarjeta inteligente.

7. Si la implementación se compone de NetScaler Gateway 10.1 - 11.0, Access Gateway 10 - 11.0, Access Gateway 9.3 o un único dispositivo Access Gateway 5.0, complete la dirección URL del servicio de autenticación de NetScaler Gateway en el cuadro URL de respuesta. StoreFront anexa automáticamente la parte estándar de la dirección URL.
   Escriba la URL internamente accesible del dispositivo. StoreFront se comunica con el servicio de autenticación de NetScaler Gateway para verificar que las solicitudes recibidas de NetScaler Gateway provienen de ese dispositivo.

Administración de dispositivos Access Gateway 5.0

Utilice la tarea Administrar dispositivos para agregar, modificar o quitar de StoreFront las direcciones IP o FQDN de los dispositivos de clúster Access Gateway 5.0.

Habilitación de la autenticación de usuario silenciosa a través de Access Controller

Utilice la tarea Habilitar autenticación silenciosa para agregar, modificar o quitar direcciones URL para el servicio de autenticación que se ejecuta en los servidores de Access Controller en el clúster de Access Gateway 5.0. Introduzca las direcciones URL de varios servidores para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. StoreFront utiliza el servicio de autenticación para realizar la autenticación de los usuarios remotos para que no necesiten volver a introducir sus credenciales cuando accedan a las tiendas.

Administración de Secure Ticket Authorities

Utilice la tarea Secure Ticket Authority para actualizar la lista de Secure Ticket Authorities (STA) de los cuales StoreFront obtiene tiquets de sesión de usuario y para configurar la fiabilidad de la sesión. El STA está alojado en servidores XenDesktop y XenApp. Emite tiquets de sesión en respuesta a las solicitudes de conexión. Estos tiquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de XenDesktop y XenApp.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo Tiendas en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una implementación de NetScaler Gateway. En el panel Acciones, haga clic en Administrar

NetScaler Gateway.

3. Haga clic en Agregar para introducir la dirección URL de un servidor que ejecuta el STA. Especifique las direcciones URL de varios servidores STA para habilitar la tolerancia de fallos; para ello, enumere los servidores por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para modificar una dirección URL, seleccione la entrada en la lista URL de Secure Ticket Authority y haga clic en Modificar. Seleccione una dirección URL en la lista y haga clic en Quitar para que StoreFront deje de recibir tiquets de sesión de ese STA.
4. Si desea que XenDesktop y XenApp mantengan abiertas las sesiones desconectadas mientras Citrix Receiver intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y desea asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tiquets de dos STA, si están disponibles.
   Cuando la casilla Solicitar tiquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tiquets de sesión de dos STA diferentes con el fin de que las sesiones de usuario no se interrumpan si un STA no está disponible durante el curso de la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.

Quitar implementaciones de NetScaler Gateway

En el panel **Acciones**, utilice la tarea Quitar en **Administrar NetScaler Gateway** para eliminar de StoreFront la información de una implementación de NetScaler Gateway. Una vez que se ha quitado una implementación de NetScaler Gateway, los usuarios ya no pueden acceder a las tiendas a través de esa implementación.

Equilibrio de carga con NetScaler

Aug 14, 2017

Este artículo contiene la información necesaria para usar NetScaler para el equilibrio de carga de dos o más servidores StoreFront.

Configuración de un grupo de servidores StoreFront y del equilibrio de carga de NetScaler

Planificación de la implementación de StoreFront con equilibrio de carga

En este artículo se ofrecen instrucciones acerca de cómo implementar un grupo de servidores StoreFront que contengan como mínimo dos servidores StoreFront en toda la configuración activa de equilibrio de carga.En el artículo se ofrece información detallada acerca de cómo configurar un dispositivo NetScaler para equilibrar la carga de solicitudes entrantes de Citrix Receiver o Citrix Receiver para Web entre todos los nodos de StoreFront del grupo de servidores. También ofrece información sobre cómo configurar el nuevo monitor de StoreFront para usarlo con un dispositivo NetScaler o un equilibrador de carga externo.

Para ver ejemplos de configuración de equilibrio de carga, consulte los apartados “Caso 1” y “Caso 2” que se ofrecen a continuación.

Probados con el siguiente entorno

- Cuatro nodos de StoreFront 3.0 de Windows Server 2012 R2 en un solo grupo de servidores.
- Un equilibrador de carga NetScaler 10.5 configurado para el equilibrio de carga con el método de menor cantidad de conexiones Least Connection y el tipo de persistencia CookieInsert.
- Un cliente de prueba Windows 8.1 con Fiddler 4.0 y Citrix Receiver para Windows 4.3 instalados.

Requisitos de certificado de servidor para la implementación con equilibrio de carga, si quiere utilizar HTTPS

Consulte la sección Planificación de uso de la puerta de enlace y el servidor de certificados.

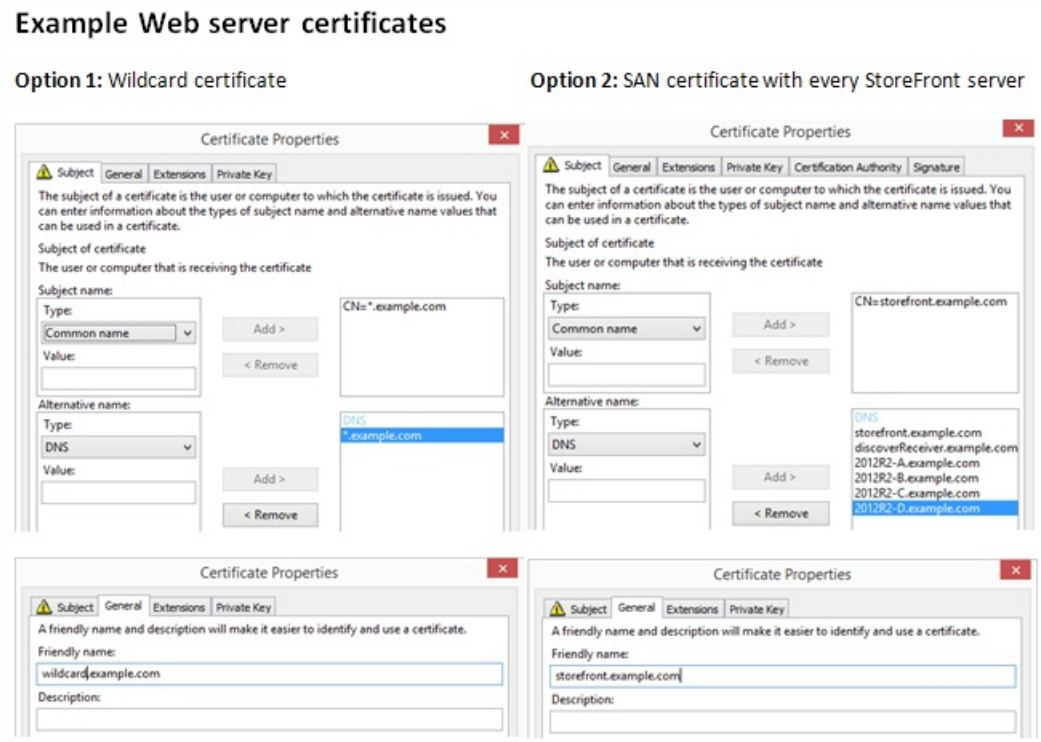
Tenga en cuenta las siguientes opciones antes de: adquirir un certificado de una entidad de certificación comercial o emitir uno de la entidad de certificación (CA) de la empresa.

- **Opción 1:** Usar un certificado comodín *.ejemplo.com en el servidor virtual de equilibrio de carga de NetScaler y en los nodos del grupo de servidores StoreFront.Esto simplifica la configuración y permite agregar más servidores StoreFront en el futuro, sin la necesidad de reemplazar el certificado.

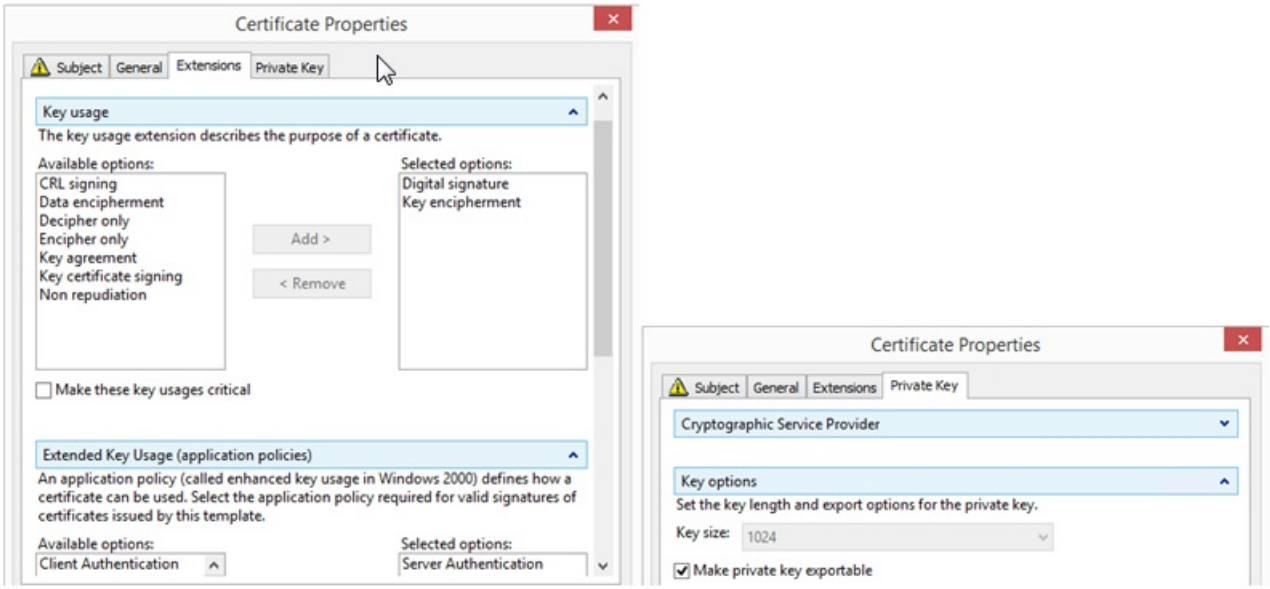
- **Opción 2:** Usar un certificado con nombres alternativos de sujeto (SAN) en el servidor virtual de equilibrio de carga de NetScaler y en los nodos del grupo de servidores StoreFront.Los nombres SAN adicionales que contenga el certificado que coincidan con todos los nombres de dominio completos (FQDN) de servidor StoreFront son opcionales aunque se recomiendan, ya que permiten una mayor flexibilidad en la implementación de StoreFront.Incluya un nombre SAN para la detección basada en correo electrónico como, por ejemplo, discoverReceiver.ejemplo.com.

  Para obtener información sobre la configuración de la detección basada en correo electrónico, consulte http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/.

Nota: Cuando no es posible exportar la clave privada asociada al certificado. Use dos certificados independientes: uno en el servidor virtual de equilibrio de carga de NetScaler y otro distinto en los nodos del grupo de servidores StoreFront. Ambos certificados deben incluir nombres alternativos de sujeto.



Common Properties



Creación de un certificado de servidor para el equilibrador de carga de NetScaler y todos los servidores StoreFront

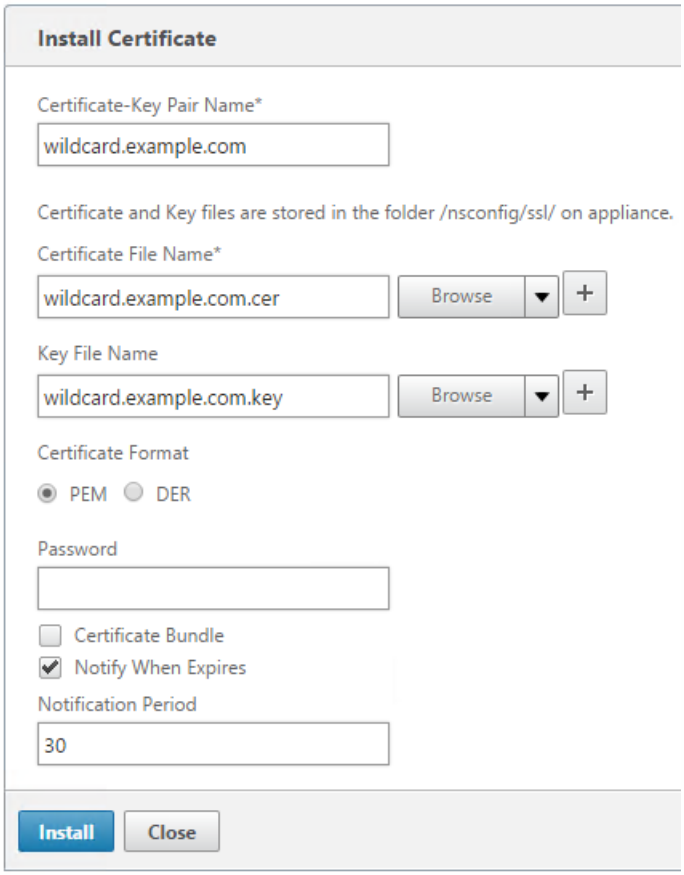
Cómo importar un certificado emitido por una entidad de certificación de Windows a un dispositivo NetScaler mediante OpenSSL

- WinSCP es una herramienta externa útil y gratuita para trasladar archivos desde una máquina con Windows a un sistema de archivos de NetScaler Gateway.Copie los certificados que quiere importar a la carpeta **/nsconfig/ssl/** del sistema de archivos de NetScaler Gateway.
- Puede usar las herramientas de OpenSSL en NetScaler Gateway para extraer el certificado y la clave de un archivo **PKCS12/PFX** y, así, crear dos archivos X.509 CER y KEY independientes en formato PEM que puede utilizar NetScaler Gateway.

1. Copie el archivo PFX a **/nsconfig/ssl**, en el dispositivo NetScaler Gateway o en VPX.
2. Abra la interfaz de línea de comandos (CLI) de NetScaler.
3. Escriba **Shell** para salir de la interfaz de línea de comandos de NetScaler y pasar al shell de FreeBSD.
4. Para cambiar de directorio, use **cd /nsconfig/ssl**.
5. Ejecute **openssl pkcs12 -in .pfx -nokeys -out .cer** y escriba la contraseña del archivo PFX cuando se le solicite.
6. Ejecute **openssl pkcs12 -in .pfx -nocerts -out .key** y escriba la contraseña del archivo PFX cuando se le solicite. A continuación, establezca la frase de contraseña para la clave privada PEM para proteger el archivo KEY.
7. Ejecute **ls –al** para comprobar que los archivos CER y KEY se han creado correctamente en **/nsconfig/ssl/**.
8. Escriba **Exit** para volver a la interfaz de línea de comandos de NetScaler.

Configuración del certificado de servidor en NetScaler después de importarlo

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione Traffic Management > SSL > SSL Certificates y haga clic en Install.
3. En la ventana Install Certificate, escriba el nombre del certificado y del par de claves privadas.
   - Seleccione el archivo de certificado .cer en el sistema de archivos de NetScaler, en /nsconfig/ssl/.
   - Seleccione, en la misma ubicación, el archivo .key que contiene la clave privada.



Creación de registros DNS para el equilibrador de carga del grupo de servidores StoreFront

Cree un registro DNS A y un registro PTR para el nombre de dominio completo compartido seleccionado.Los clientes de la red usarán este nombre de dominio completo para acceder al grupo de servidores StoreFront mediante el equilibrador de carga de NetScaler.

Ejemplo: **storefront.ejemplo.com** representa la dirección IP virtual (VIP) del servidor virtual de equilibrio de carga.

Caso 1: Una conexión segura de extremo a extremo HTPPS 443 entre el cliente y el equilibrador de carga de NetScaler y también entre el equilibrador de carga y dos o más servidores StoreFront 3.0.

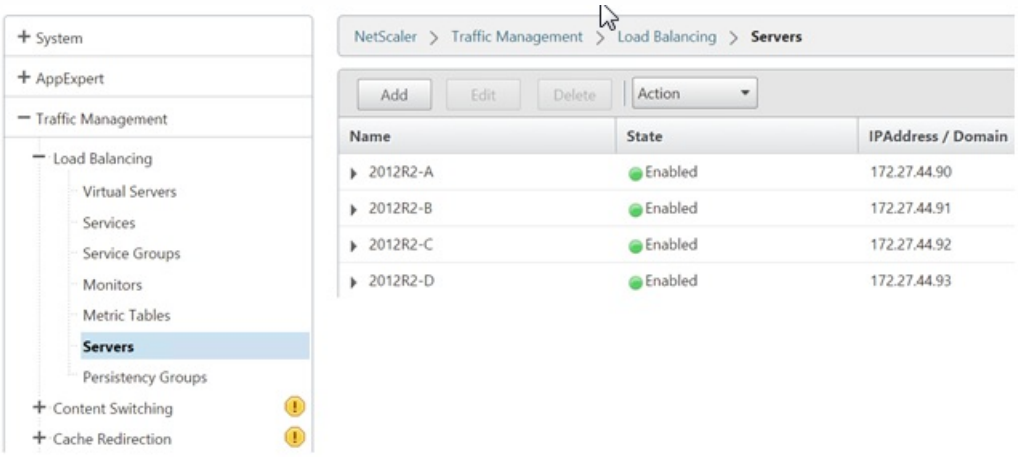
En este caso, se usa un monitor de StoreFront modificado, a través del puerto 443.

Cómo agregar nodos de servidor StoreFront individuales al equilibrador de carga de NetScaler

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione **Traffic Management > Load Balancing > Servers > Add** y agregue cada uno de los cuatro nodos de StoreFront cuyas cargas quiere equilibrar.

   Por ejemplo = 4 x 2012R2 nodos de StoreFront llamados 2012R2 A - D

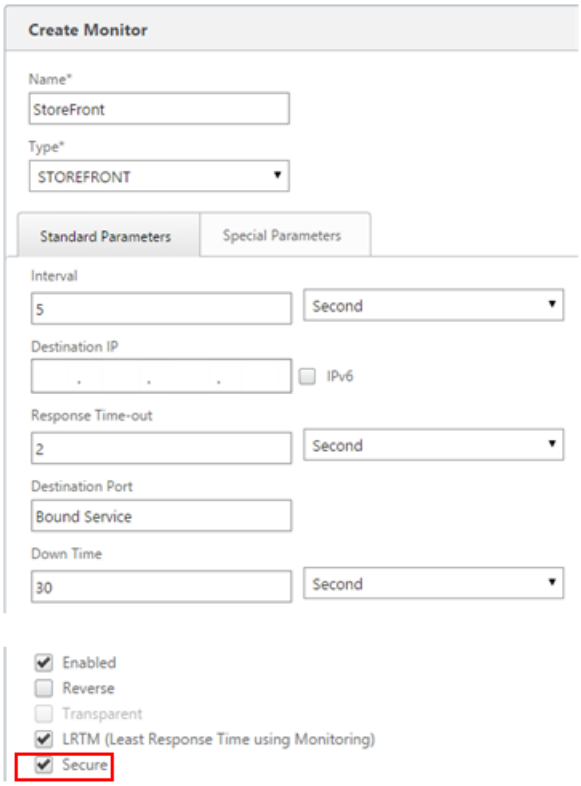
3. Use una configuración de servidor basada en IP y especifique la dirección IP del servidor de cada nodo de StoreFront.



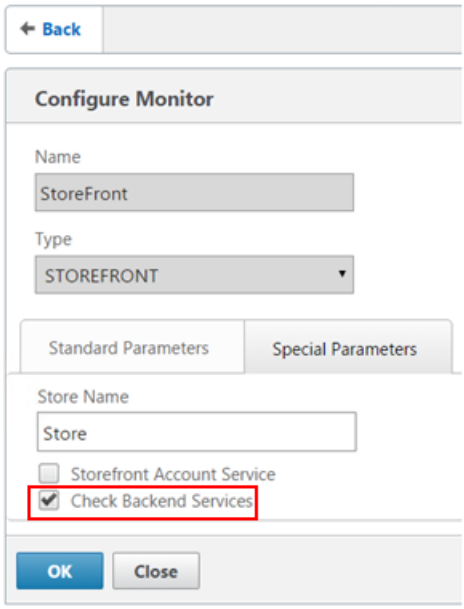
Cómo definir un monitor de StoreFront para comprobar el estado de todos los nodos de StoreFront en el grupo de servidores

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione **Traffic Management > Load Balancing > Monitors > Add** y agregue un nuevo monitor llamado StoreFront. A continuación, acepte todos los valores predeterminados.
3. En el menú desplegable **Type**, seleccione **StoreFront**.
4. Compruebe que la casilla **Secure** está marcada si se utilizan conexiones SSL entre el servidor virtual de equilibrio de carga y StoreFront; de lo contrario, deje esta opción desmarcada.
5. Especifique el nombre de la tienda en la ficha de parámetros especiales.
6. Marque la casilla de verificación **Check Backend Services** en la ficha de parámetros especiales.Esta opción permite supervisar los servicios que se ejecuten en el servidor StoreFront.Los servicios de StoreFront se supervisan por sondeo de un servicio Windows que se ejecuta en el servidor StoreFront, el cual devuelve el estado de todos los servicios de StoreFront en ejecución.

Standard Parameters Tab



Special Parameters Tab

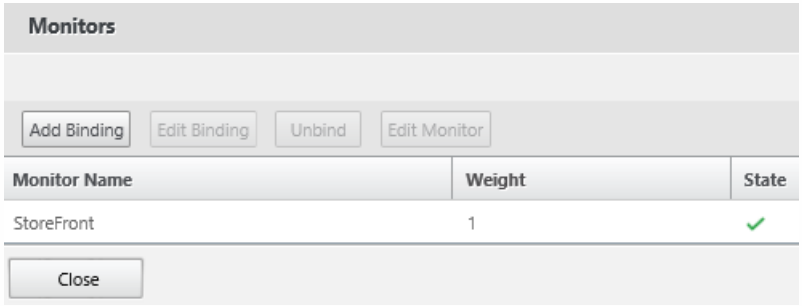


Cómo crear un grupo de servicios HTTPS 443 que contenga todos los servidores StoreFront

1. En el grupo de servicios, seleccione la opción de miembros en el lado derecho y agregue todos los nodos de servidor StoreFront que ha definido previamente en el apartado de servidores.

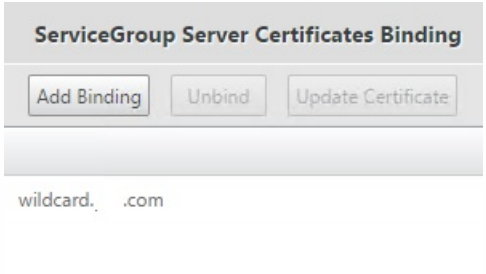
2. Configure el puerto SSL y adjudique a cada nodo un ID de servidor único al agregarlos.

3. En la ficha Monitors, seleccione el monitor de StoreFront que ha creado anteriormente.



4. En la ficha Certificates, enlace el certificado de servidor que ha importado anteriormente.

5. Enlace el certificado de CA usado para firmar el certificado de servidor que ha importado antes, así como cualquier otra entidad de certificación (CA) que pueda formar parte de la cadena de confianza de la infraestructura de clave pública (PKI).

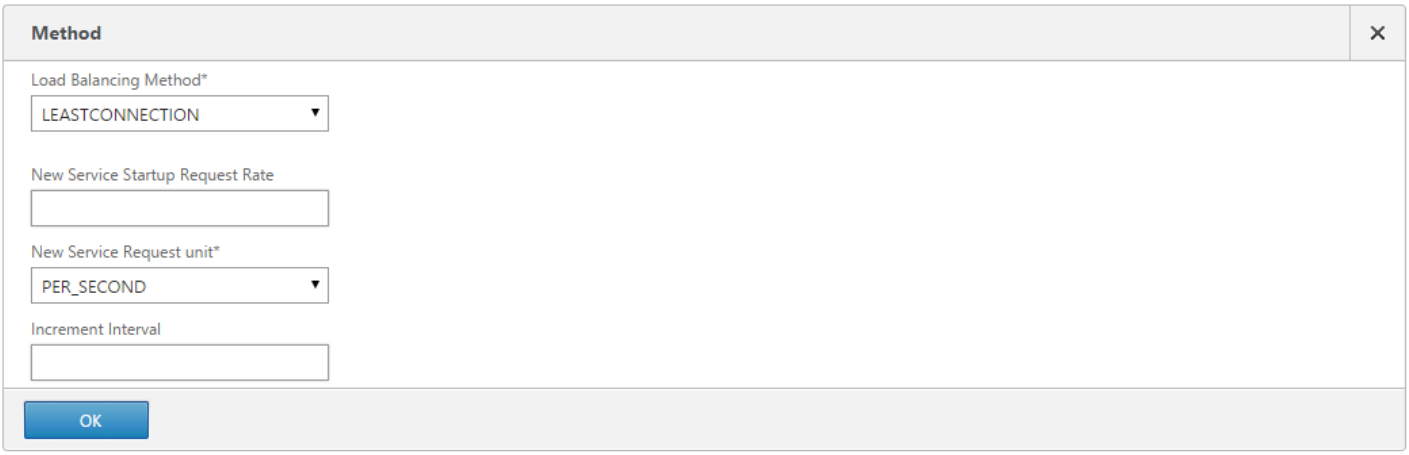


Cómo crear un servidor virtual de equilibrio de carga para el tráfico del usuario

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.

2. Seleccione **Traffic Management > Load Balancing > Virtual Servers > Add** para crear un nuevo servidor virtual.

3. Seleccione un método de equilibrio de carga para el servidor virtual.Las opciones más comunes para el equilibrio de carga de StoreFront son **round robin** o **least connection**.



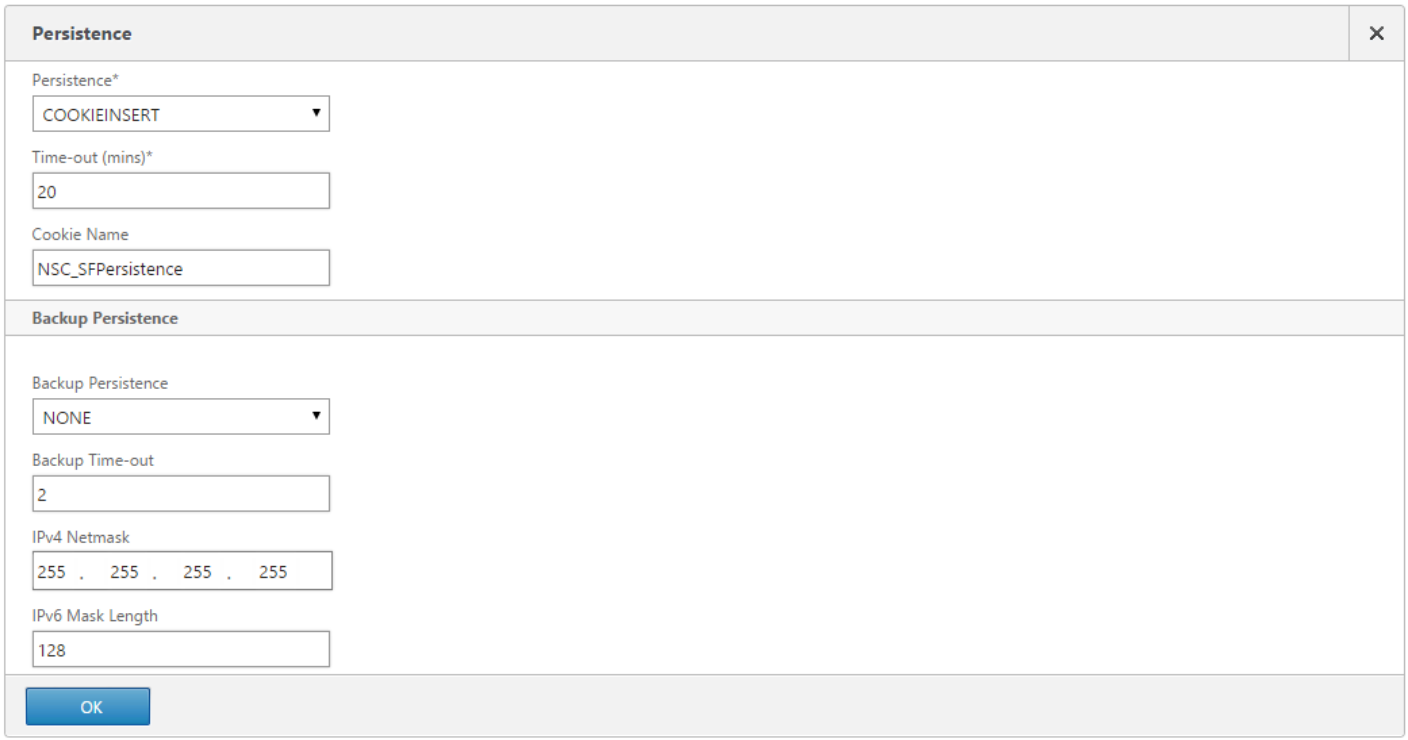
4. Vincule el **grupo de servicios** que ha creado anteriormente al servidor virtual de equilibrio de carga.

5. Enlace el mismo certificado de servidor y de CA (que ya ha enlazado al grupo de servicio) al servidor virtual de equilibrio de carga.

6. Desde el menú del servidor virtual de equilibrio de carga, seleccione la persistencia (**Persistence**) en el lado derecho y establezca el método de persistencia en **CookieInsert**.

7. Dé un nombre a la cookie. Por ejemplo, **NSC_SFPersistence**, ya que esto facilita identificar en Fiddler los rastros durante la depuración.

8. Establezca la persistencia de respaldo en **None**.



Caso 2: Terminación HTTPS; comunicación HTTPS 443 entre el cliente y el equilibrador de carga de NetScaler, y conexiones HTTP 80 entre el equilibrador de carga y los servidores StoreFront 3.0 detrás de él.

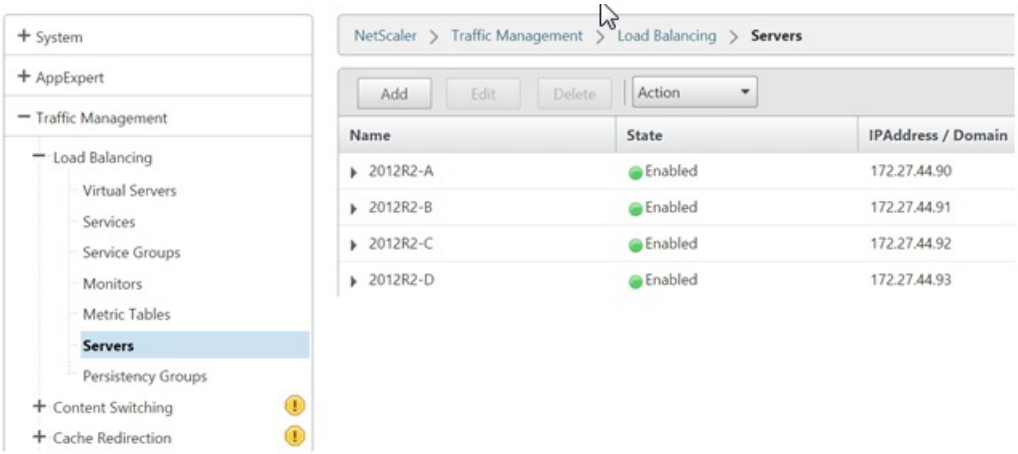
En este caso, se usa el monitor predeterminado de StoreFront a través del puerto 8000.

Cómo agregar uno o varios servidores StoreFront al equilibrador de carga de NetScaler

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione **Traffic Management > Load Balancing > Servers > Add** y agregue cada uno de los cuatro servidores de StoreFront cuyas cargas quiere equilibrar.

   Por ejemplo = 4 x 2012R2 servidores StoreFront llamados 2012R2 A - D

3. Use una configuración de servidor basada en IP y especifique la dirección IP del servidor de cada servidor StoreFront.



Cómo definir un monitor de StoreFront HTTP 8000 para comprobar el estado de todos los servidores StoreFront en el grupo de servidores

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione **Traffic Management > Monitors > Add** y agregue un nuevo monitor llamado StoreFront.
3. Agregue un nombre para el nuevo monitor y acepte los valores predeterminados.
4. Seleccione **StoreFront** desde el menú desplegable **Type**.
5. Especifique el nombre de la tienda en la ficha de parámetros especiales.
6. Escriba **8000** en el puerto de destino, ya que coincide con la instancia de monitor predeterminada que se crea en cada servidor StoreFront.
7. Marque la casilla **Check Backend Services** en la ficha de parámetros especiales.Esta opción permite supervisar los servicios que se ejecuten en el servidor StoreFront.Los servicios de StoreFront se supervisan por sondeo de un servicio Windows que se ejecuta en el servidor StoreFront, el cual devuelve el estado de todos los servicios de StoreFront en ejecución.

Cómo crear un grupo de servicios HTTP 80 que contenga todos los servidores StoreFront

1. En el grupo de servicios, seleccione la opción de miembros en el lado derecho y agregue todos los nodos de servidor StoreFront que ha definido previamente en el apartado de servidores.
2. Establezca el puerto HTTP en 80 y adjudique a cada servidor un ID de servidor único al agregarlos.
3. En la ficha Monitors, seleccione el monitor de StoreFront que ha creado anteriormente.

Creación de un servidor virtual de equilibrio de carga de terminación HTTPS para el tráfico de usuarios

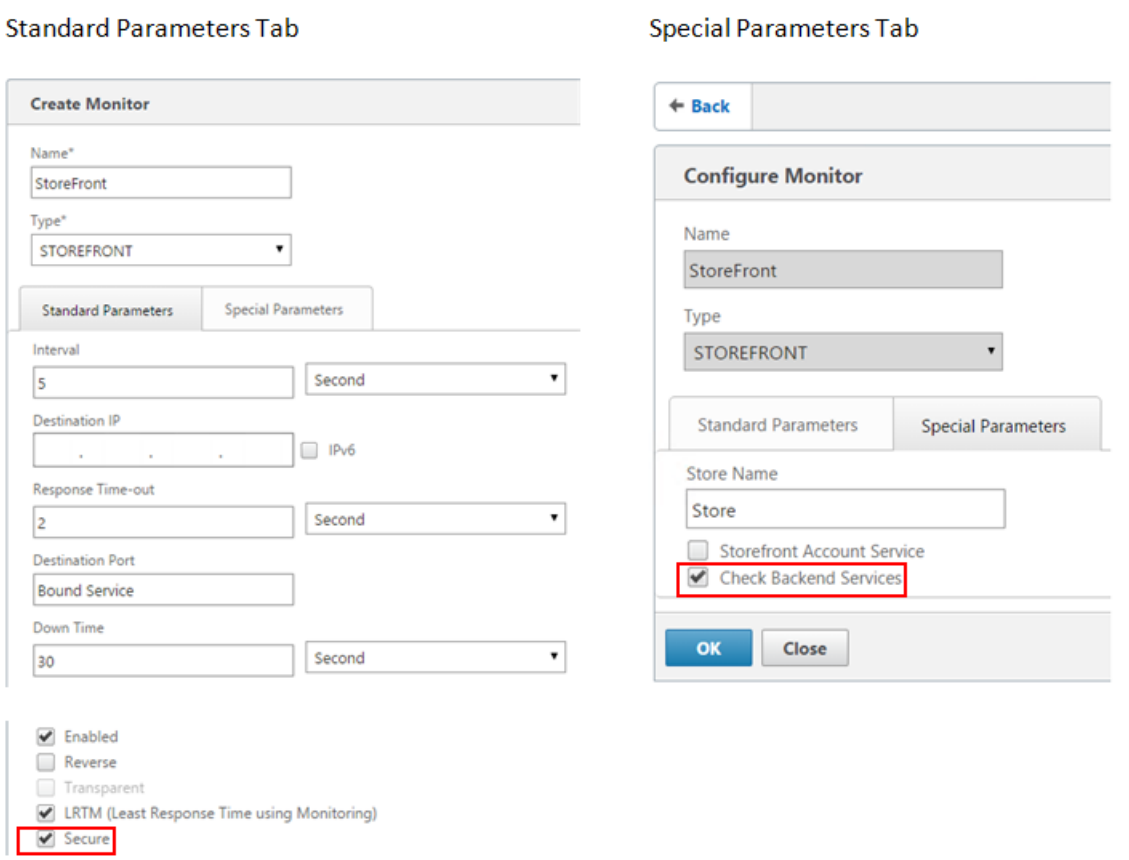
1. Seleccione **Traffic Management > Load Balancing > Virtual Servers > Add** para crear un nuevo servidor virtual.
2. Seleccione un método de equilibrio de carga para el servidor virtual.Las opciones más comunes para el equilibrio de carga de StoreFront son **round robin** o **least connection**.
3. Vincule el **grupo de servicios** que ha creado anteriormente al servidor virtual de equilibrio de carga.
4. Enlace el mismo certificado de servidor y de CA (que ya ha enlazado al grupo de servicio) al servidor virtual de equilibrio de carga.

   Nota: Si no se permite que el cliente almacene la cookie HTTP, las solicitudes subsiguientes no contienen la cookie HTTP y no se usará la **persistencia**.

5. Desde el menú del servidor virtual de equilibrio de carga, seleccione **Persistence** y establezca el método de persistencia

en **CookieInsert**.

6. Nombre de la cookie. Por ejemplo, **NSC_SFPersistence**, ya que esto facilita identificar en Fiddler los rastros durante la depuración.
7. Establezca la persistencia de respaldo en **None**.



Creación de un servidor virtual de equilibrio de carga para la sincronización de suscripciones entre grupos de servidores

Entre los aspectos a tener en cuanta antes de crear un servidor virtual de equilibrio de carga, se incluyen los siguientes:

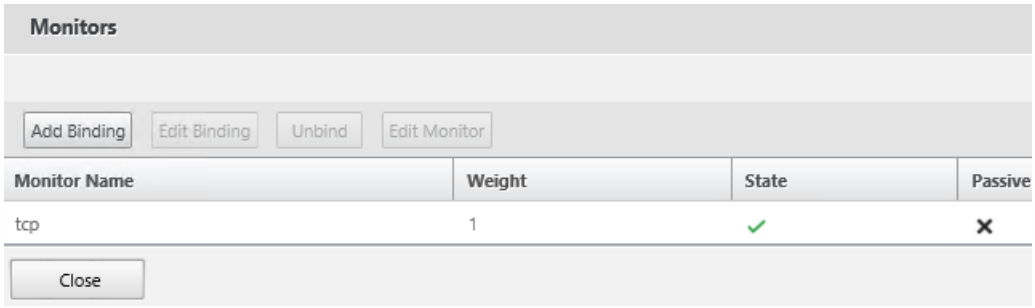
- **Opción 1:** Crear un servidor virtual único para equilibrar la carga solamente del tráfico de usuarios.Esto es todo lo que se necesita si se realizan únicamente inicios ICA de aplicaciones y escritorios publicados (todo lo que se precisa obligatoriamente y en condiciones normales).
- **Opción 2:** Crear un par de servidores virtuales: uno para equilibrar la carga del tráfico de usuarios para realizar inicios ICA de aplicaciones y escritorios publicados, y otro para equilibrar la carga de las operaciones de sincronización de los datos de suscripción (opción necesaria solo cuando se propaguen datos de suscripción entre dos o más grupos de servidores StoreFront con carga equilibrada que formen parte de una implementación a gran escala que contenga múltiples sitios).

Si una implementación a gran escala de múltiples sitios consta de dos o más grupos de servidores StoreFront que se encuentran en zonas geográficas distintas, puede replicar los datos de suscripción entre ellos mediante una estrategia de extracción que siga una programación periódica. La replicación de datos de suscripción de StoreFront utiliza el puerto TCP 808, por lo que utilizar un servidor virtual existente de equilibrio de carga en el puerto HTTP 80 o HTTPS 443 da error. Para una alta disponibilidad en este servicio, cree un segundo servidor virtual en cada dispositivo NetScaler de la implementación. De esta manera, equilibrará la carga en el puerto TCP 808 proveniente de cada grupo de servidores StoreFront. Cuando

configure la programación de la replicación, especifique la dirección de un grupo de servidores que coincida con la dirección IP del servidor virtual de sincronización de suscripciones. Compruebe que la dirección del grupo de servidores es el nombre de dominio completo (FQDN) del equilibrador de carga para el grupo de servidores en esa ubicación.

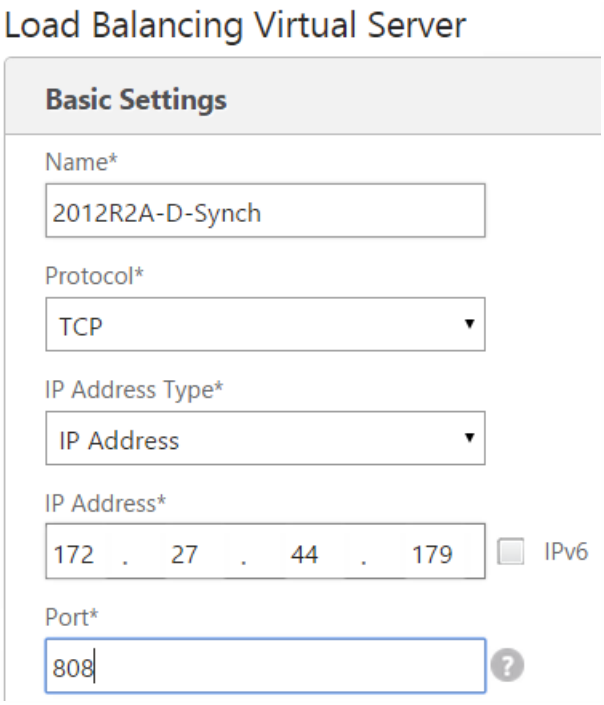
Configuración de un grupo de servicios para la sincronización de suscripciones

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione **Traffic Management > Service Groups > Add** y agregue un nuevo grupo de servicios.
3. Cambie el protocolo a **TCP**.
4. En el grupo de servicios, seleccione la opción **Members** en el lado derecho y agregue todos los nodos de servidor StoreFront que ha definido previamente en el apartado de servidores.
5. En la ficha **Monitors**, seleccione el monitor de TCP.



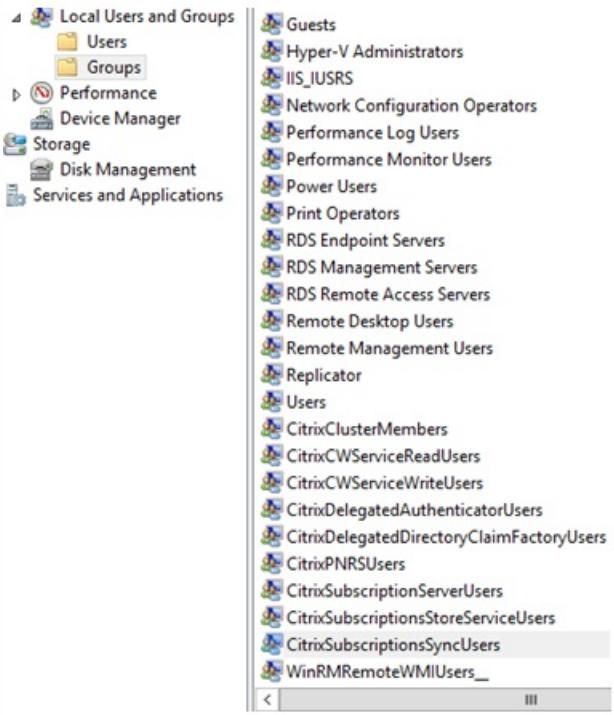
Creación de un servidor virtual de equilibrio de carga para la sincronización de suscripciones entre grupos de servidores

1. Inicie sesión en la interfaz gráfica de usuario de administración de NetScaler.
2. Seleccione **Traffic Management > Service Groups > Add** y agregue un nuevo grupo de servicios.
3. Establezca el método de equilibrio de carga en **round robin**.
4. Cambie el protocolo a **TCP**.
5. Escriba **808** (no **443**) como número de puerto.



Pertenencia al grupo CitrixSubscriptionsSyncUsers

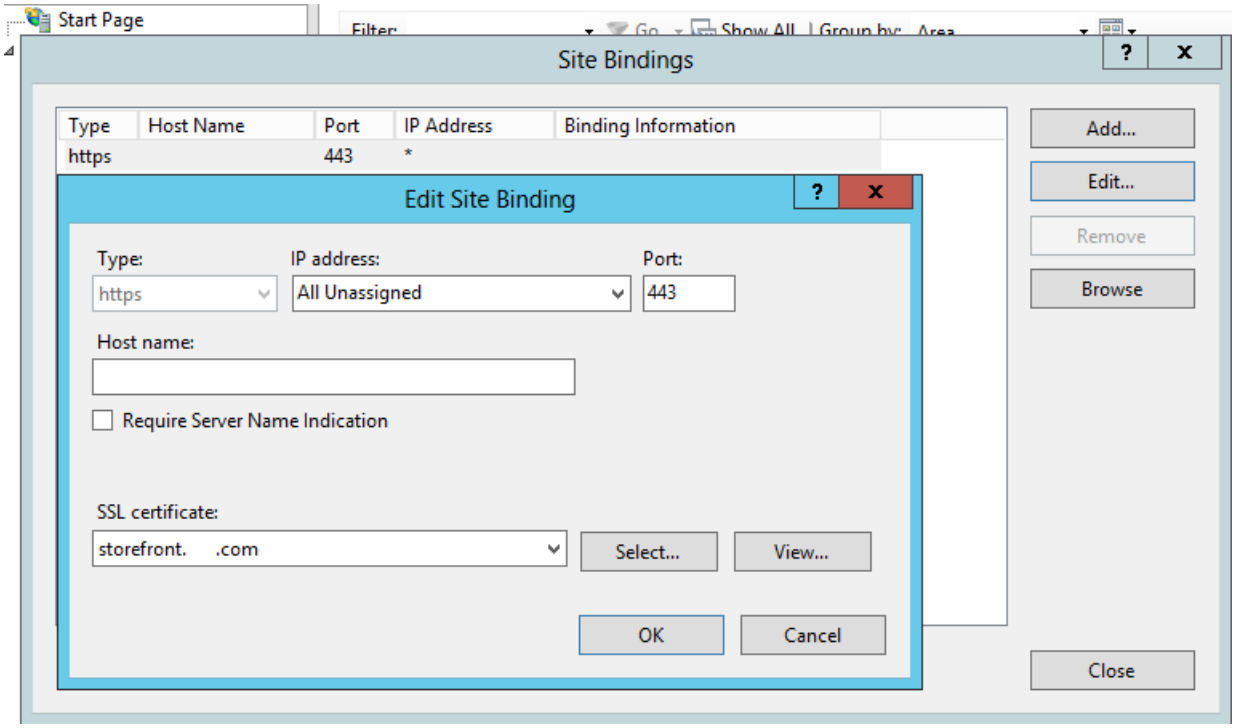
Para que el **servidor StoreFront A** en la **Ubicación A** solicite y extraiga datos de suscripción del **servidor B** en otra ubicación, el servidor A debe ser miembro del grupo de seguridad local **CitrixSubscriptionsSyncUsers** del servidor B. El grupo local **CitrixSubscriptionsSyncUsers** contiene una lista de control de acceso de todos los servidores StoreFront remotos autorizados a extraer datos de suscripción de un servidor determinado.Para una sincronización bidireccional de suscripciones (es decir, que el servidor B extraiga datos de suscripción del servidor A), el servidor B también debe ser miembro del grupo de seguridad **CitrixSubscriptionsSyncUsers** en el servidor A.



Configuración del grupo de servidores StoreFront para el equilibrio de carga

1. Importe en cada nodo de StoreFront existente del grupo de servidores el mismo certificado y la misma clave privada que se implementaron en el servidor virtual de NetScaler de equilibrio de carga.

2. Cree un enlace HTTPS en IIS en cada nodo de StoreFront y, a continuación, vincúlele el certificado importado anteriormente.



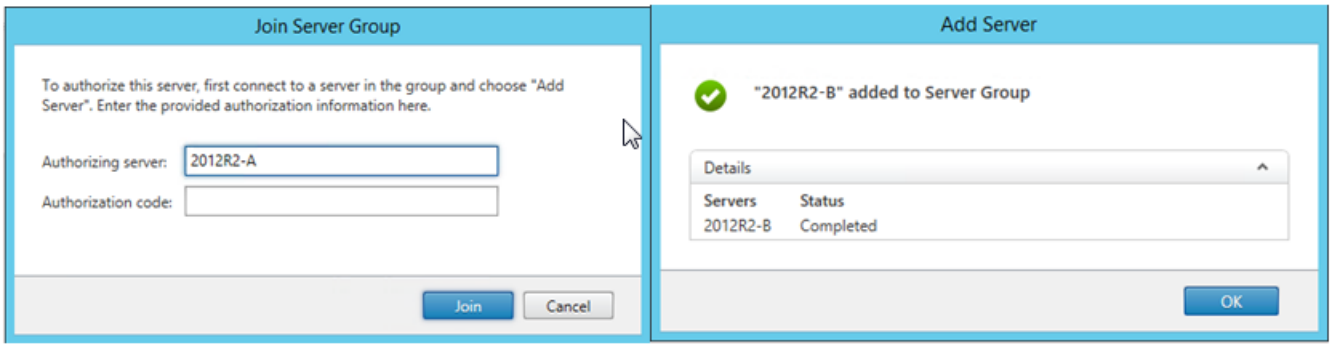
3. Instale StoreFront en cada nodo del grupo de servidores.

4. Durante la instalación de StoreFront, establezca la URL base del host en el nodo principal que será el nombre de dominio completo (FQDN) compartido que utilizarán todos los miembros del grupo de servidores.Debe usar un certificado que contenga el FQDN de equilibrio de carga como un nombre común (CN) o como nombre alternativo de sujeto (SAN).

Consulte Creación de un certificado SSL para el equilibrador de carga de NetScaler y los servidores StoreFront.

5. Cuando complete la configuración inicial de StoreFront, incorpore cada nodo (uno tras otro) al grupo de servidores mediante el nodo principal.

6. Seleccione **Grupo de servidores > Agregar servidor > Copie el código de autorización** en el servidor que se une al grupo.



7. Propague la configuración desde el nodo principal a todos los demás nodos del grupo de servidores.

8. Pruebe el grupo de servidores con carga equilibrada mediante un cliente que pueda contactar y resolver el nombre de dominio completo (FQDN) compartido del equilibrador de carga.

Citrix Service Monitor

Para habilitar la supervisión externa del estado de ejecución de los servicios Windows en los que se basa el funcionamiento correcto de StoreFront, use el servicio Windows de **Citrix Service Monitor**.Este servicio no tiene otras dependencias de servicio, y puede supervisar y notificar errores de otros servicios importantes de StoreFront.El monitor permite que el estado relativo de las implementaciones de servidores StoreFront se determine de forma externa con la ayuda de otros componentes de Citrix como, por ejemplo, NetScaler.Un software de terceros puede consumir la respuesta XML del monitor de StoreFront para supervisar el estado de los servicios esenciales de StoreFront.

Una vez implementado StoreFront, se crea un monitor predeterminado que usa HTTP y el puerto 8000.

Nota: Solo puede existir una instancia de monitor en una implementación de StoreFront.

Para realizar cambios en el monitor predeterminado existente (como cambiar el protocolo y el puerto a HTTPS 443), utilice los siguientes tres cmdlets de PowerShell para ver o cambiar la configuración de la URL del servicio de monitor de StoreFront.

Quite el monitor de servicios (Service Monitor) predeterminado y reemplácelo por uno que use HTTPS y el puerto 443.

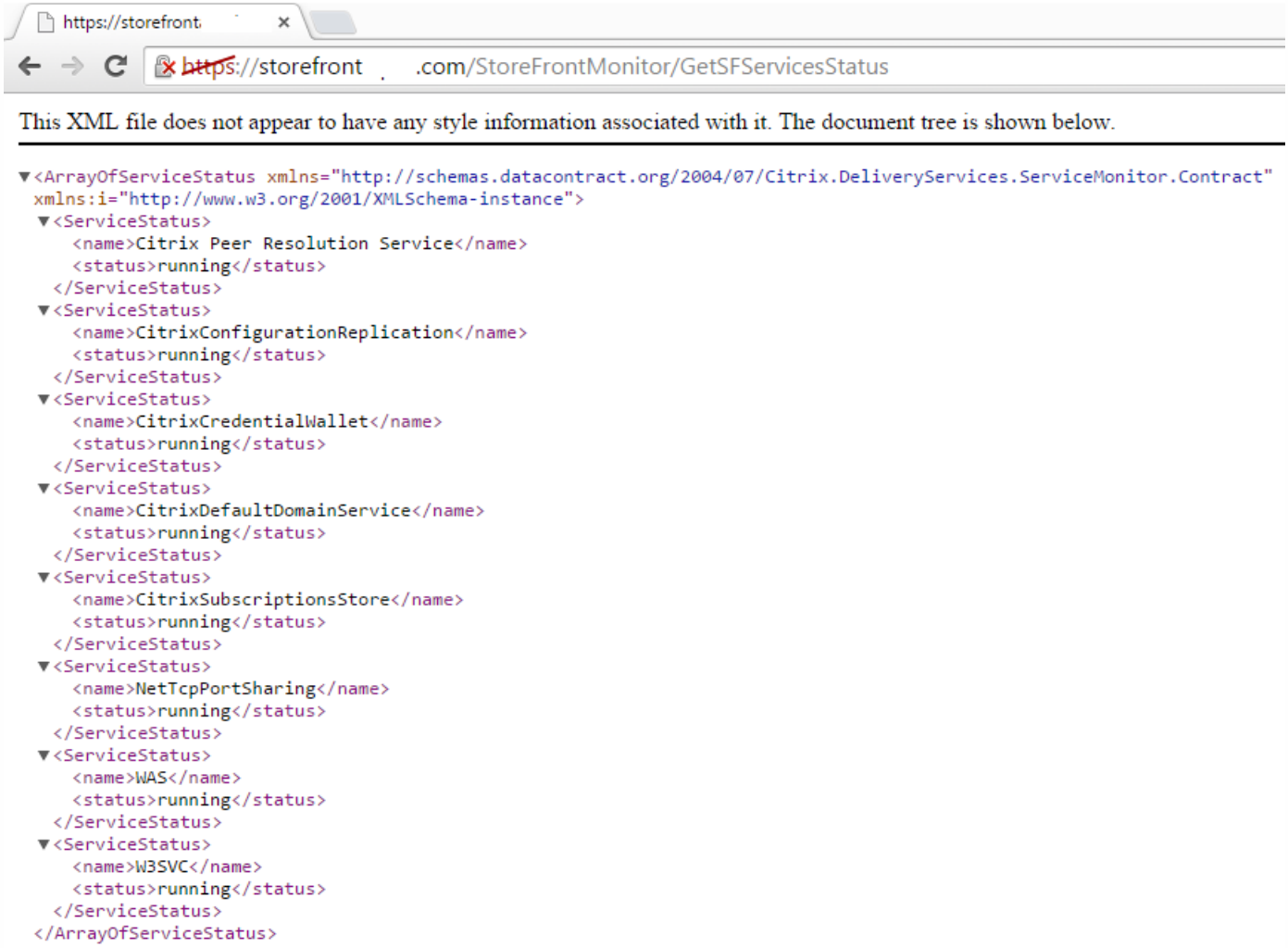
1. Abra el entorno Integrated Scripting Environment (ISE) de PowerShell en el servidor StoreFront principal y ejecute los comandos siguientes para cambiar el monitor predeterminado a HTTPS 443.

```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"

Set-STFServiceMonitor -ServiceUrl $ServiceUrl

Get-STFServiceMonitor
```

2. Una vez completada la operación, propague los cambios a los demás servidores del grupo de servidores StoreFront.

3. Para realizar una prueba rápida en el nuevo monitor, introduzca la URL siguiente en el explorador Web presente en el servidor StoreFront, o en cualquier otra máquina con acceso de red al servidor StoreFront.El explorador debería devolver un resumen XML del estado de cada servicio de StoreFront.

https://:443/StoreFrontMonitor/GetSFServicesStatus

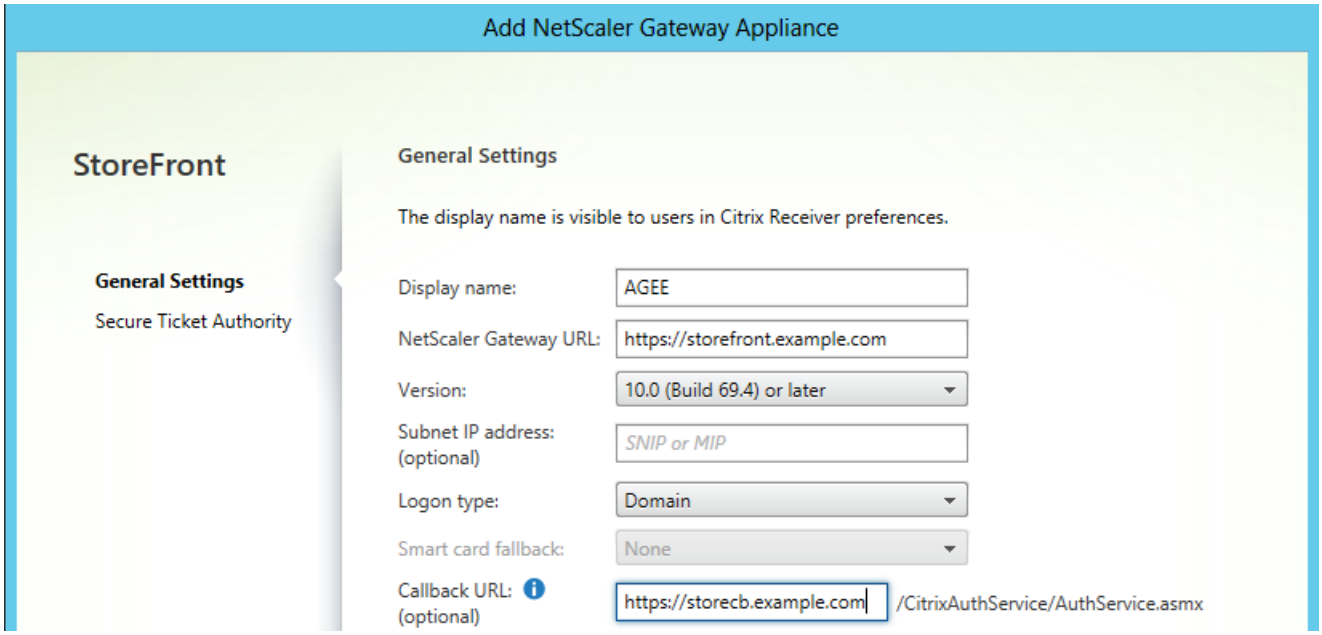


NetScaler Gateway y servidores virtuales de equilibrio de carga en el mismo dispositivo NetScaler

Si ha configurado el servidor virtual de NetScaler Gateway y el servidor virtual de equilibrio de carga en el mismo dispositivo NetScaler, los usuarios del dominio interno pueden tener problemas al intentar acceder directamente a la URL base del host StoreFront con carga equilibrada en lugar de pasar por el servidor virtual de NetScaler Gateway.

En este caso, StoreFront asume que el usuario final ya se ha autenticado en NetScaler Gateway, ya que StoreFront correlaciona la dirección IP de origen del usuario entrante con la dirección IP de subred (SNIP) de NetScaler Gateway. Por eso, StoreFront intenta usar el protocolo AGBasic para realizar la autenticación silenciosa de NetScaler Gateway, en lugar de solicitar realmente al usuario que inicie sesión con sus credenciales de dominio.Para evitar este problema, omita la dirección SNIP como se muestra más abajo, de modo que se use autenticación con nombre de usuario y contraseña en lugar de AGBasic.

Configuración de un NetScaler Gateway en el grupo de servidores StoreFront



Opciones de bucle invertido al equilibrar la carga de un grupo de servidores StoreFront mediante NetScaler

En versiones anteriores de StoreFront (como 2.6 o versiones anteriores), Citrix recomendaba modificar manualmente el archivo de hosts en cada servidor StoreFront para asignar el nombre de dominio completo (FQDN) del equilibrador de carga a la dirección de bucle o la dirección IP del servidor StoreFront concreto.Esto garantiza que Receiver para Web siempre se comunique con los servicios de StoreFront en el mismo servidor en una implementación con equilibrio de carga.Esto es necesario porque se crea una sesión HTTP durante el proceso de inicio de sesión explícito entre Receiver para Web y el servicio de autenticación, y Receiver para Web se comunica con los servicios de StoreFront usando el nombre FQDN base.Si este nombre se resolviera en el equilibrador de carga, el equilibrador podría enviar el tráfico a otro servidor StoreFront del grupo, lo que puede provocar un error de autenticación.Esto no circunvala el equilibrador de carga excepto cuando Receiver para Web intenta conectar con el servicio de StoreFront que reside en su mismo servidor.

Puede definir opciones de bucle usando PowerShell.Si habilita el bucle invertido, ya no tendrá que crear entradas del archivo de host en cada servidor StoreFront del grupo de servidores.

Ejemplo de archivo web.config de Receiver para Web:

Ejemplo de comando de PowerShell:

& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.ps1"

Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "OnUsingHttp" -LoopbackPortUsingHttp 81

El parámetro **-Loopback** puede tomar tres valores posibles.

Valor	Contexto
En: Cambia el host de la URL a 127.0.0.1.El esquema y el puerto (si se especificó) no se modifican.	No se puede usar si se utiliza un equilibrador de carga con terminación SSL.

OnUsingHttp: Cambia el host a 127.0.0.1, el esquema a HTTP y modifica el valor del puerto configurado en el atributo **loopbackPortUsingHttp**.	Úselo solo cuando el equilibrador de carga tiene terminación SSL.La comunicación entre el equilibrador de carga y los servidores StoreFront se establece por HTTP.Puede configurar explícitamente el puerto HTTP mediante el atributo -loopbackPortUsingHttp.
Off: La URL de la solicitud no se modifica.	Úsela para la solución de problemas.Las herramientas como Fiddler no pueden capturar el tráfico entre Receiver para Web y servicios de StoreFront si el bucle invertido está establecido en "On".

Configuración de dos direcciones URL para un mismo NetScaler Gateway

Aug 14, 2017

En StoreFront, puede agregar una dirección de URL de NetScaler Gateway desde la consola de administración de StoreFront, con la opción Administrar NetScaler Gateway > Agregar o Modificar. También es posible agregar una URL de NetScaler Gateway pública y una URL de equilibrio de carga global de servidores (GSLB) en Administrar NetScaler Gateway > Importar desde un archivo.

Este artículo, muestra cómo usar los cmdlets de PowerShell y el SDK de PowerShell de StoreFront para usar un parámetro optativo, - gslburl, para establecer el atributo GslbLocation de una puerta de enlace. Esta funcionalidad simplifica la administración de NetScaler Gateway en StoreFront en los siguientes casos de uso:

1. **GSLB y varios NetScaler Gateway**. Use GSLB y varios NetScaler Gateway para equilibrar la carga de conexiones remotas con recursos publicados en dos o más ubicaciones dentro de una implementación de Citrix global de gran tamaño.
2. **NetScaler Gateway único con una URL pública o privada**. Use el mismo NetScaler Gateway para el acceso externo usando una URL pública, y para el acceso interno, usando una URL privada.

Esta es una funcionalidad avanzada. Si no está familiarizado con GSLB (Global Server Load Balancing), consulte los enlaces de información relacionada, al final de este artículo.

Esta funcionalidad ofrece las ventajas siguientes:

- Respaldo para dos URL simultáneas para un mismo objeto de puerta de enlace.
- Los usuarios pueden alternar entre dos direcciones URL diferentes para acceder a NetScaler Gateway sin que el administrador vuelva a configurar el objeto de puerta de enlace de StoreFront para que coincida con la URL de puerta de enlace que el usuario desea usar.
- Periodos de instalación y prueba más cortos, para validar la configuración de la puerta de enlace de StoreFront cuando se usan varias puertas de enlace con GSLB.
- Utilizar el mismo objeto de NetScaler Gateway en StoreFront dentro de la zona DMZ tanto para el acceso interno como el externo.
- Respaldo de ambas direcciones URL para un enrutamiento de la puerta de enlace óptimo. Para obtener más información sobre el enrutamiento óptimo de puertas de enlace, consulte Configuraciones de tienda multisitio con alta disponibilidad.

Consideraciones sobre la implementación cuando se usan dos direcciones URL de puerta de enlace

> ### Important
>
> Antes de configurar una segunda dirección URL de puerta de enlace mediante el parámetro - gslburl, Citrix recomienda consultar los certificados de servidor con los que se cuenta y cómo se lleva a cabo la resolución de DNS en la organización. Las direcciones URL que se quieran usar en la implementación de NetScaler y StoreFront deben estar presentes en los certificados del servidor. Para obtener más información sobre certificados de servidor, consulte Planificación de uso de la puerta de enlace y el servidor de certificados.

DNS

- **DNS dividida**. Las empresas grandes con frecuencia usan infraestructuras de DNS dividido. El DNS dividido implica el uso de espacios de nombres diferentes y servidores DNS diferentes y resolución DNS privada. Compruebe si tiene la infraestructura DNS existente para respaldar esto.
- **Una misma URL para el acceso interno y externo a los recursos publicados**. Decida si desea utilizar la misma dirección URL para acceder a recursos publicados desde fuera y desde dentro de la red corporativa, o considere si la posibilidad de tener direcciones URL distintas sería aceptable: por ejemplo: ejemplo.com y ejemplo.net.

Ejemplos de certificado de servidor

Esta sección contiene ejemplos de implementaciones de certificado de servidor cuando se usan dos direcciones URL de puerta de enlace.

- **Ejemplo de certificado de servidor para una implementación de StoreFront con equilibrio de carga**

  Un certificado de servidor comodín firmado de forma privada debe contener el nombre FQDN *. storefront.example.net.

  O bien:

  Un certificado de servidor SAN firmado de forma privada debe contener todos los FQDN necesarios para equilibrar la carga de tres servidores StoreFront.

  loadbalancer.storefront.example.net

  server1.storefront.example.net

  server2.storefront.example.net

  server3.storefront.example.net

  Establezca la URL base del host del grupo de servidores StoreFront para que sea el nombre FQDN compartido, que se resuelve con la dirección IP del equilibrador de carga.

  loadbalancer.storefront.example.net

- **Ejemplo de certificado de servidor para un grupo de Delivery Controllers de XenApp y XenDesktop 7.x**

  Un certificado de servidor comodín firmado de forma privada debe contener el nombre FQDN *.xendesktop.example.net.

  O bien:

  Un certificado de servidor SAN firmado de forma privada debe contener todos los nombres FQDN de servidores necesarios para un sitio de XenDesktop que contenga cuatro Controllers.

  XD1A. XenDesktop.example.NET

  XD1B. xendesktop.example.net

  XD2A. XenDesktop.example.NET

  XD2B. xendesktop.example.net

- **Ejemplo de certificado de servidor para un dispositivo NetScaler Gateway al que se accede de forma externa e**

interna, usando DNS dividido

Un certificado de servidor SAN firmado públicamente para el acceso interno y externo debe contener los nombres FQDN interno y externo.

gateway.example.com

gateway.example.net

- **Ejemplo de certificado de servidor para todas las puertas de enlace con GSLB a las que se accede externamente**

  Un certificado de servidor SAN firmado públicamente para el acceso externo a través de GSLB debe contener los nombres FQDN.

  gslbdomain.example.com

  emeagateway.example.com

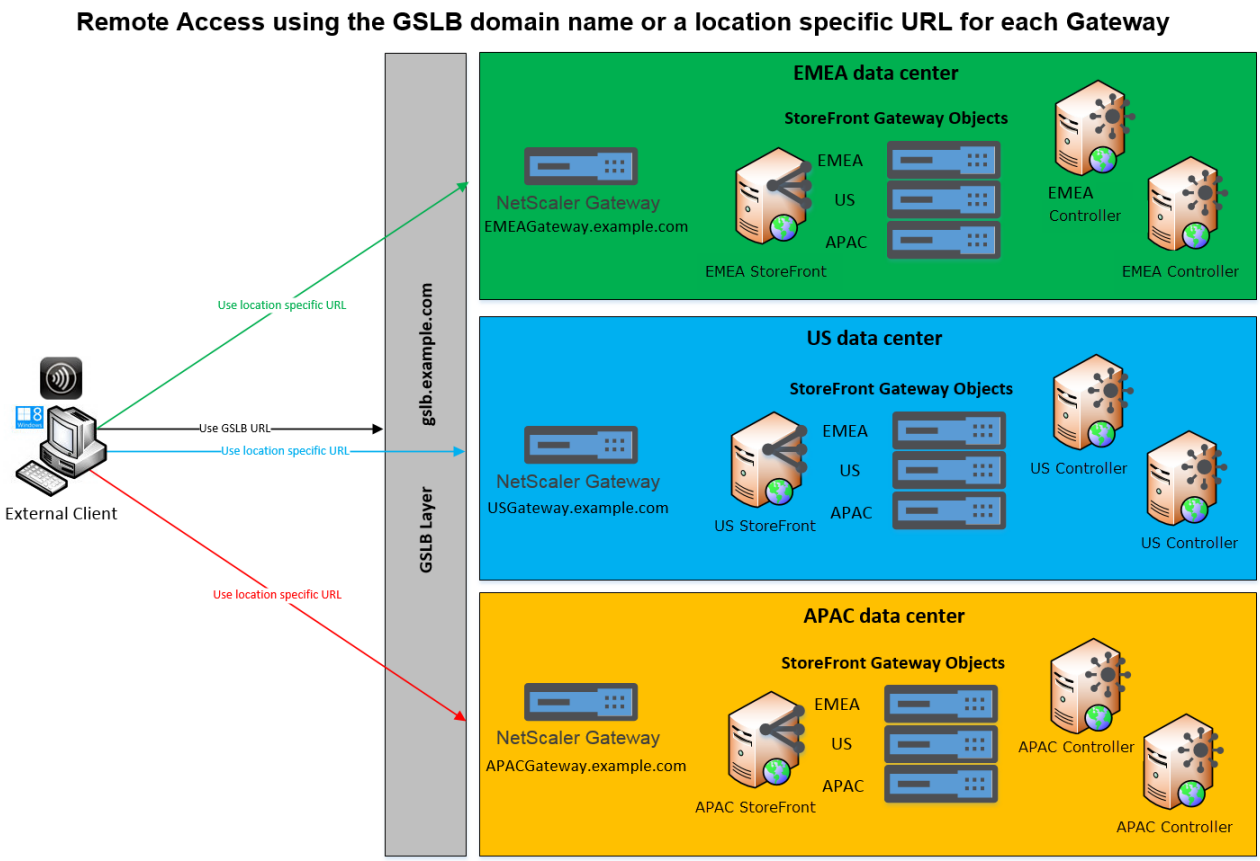
  usgateway.example.com

  apacgateway.example.com

  Esto permite al usuario acceder a la puerta de enlace más cercana usando GSLB o elegir una puerta de enlace en la ubicación que desee usando su nombre FQDN exclusivo.

Caso #1: GSLB y varios NetScaler Gateways

El administrador usa el equilibrio de carga de servidores global (GSLB) y varias puertas de enlace NetScaler Getwway para equilibrar las conexiones remotas con recursos publicados en dos o más ubicaciones, dentro de una implementación de Citrix global de gran tamaño.

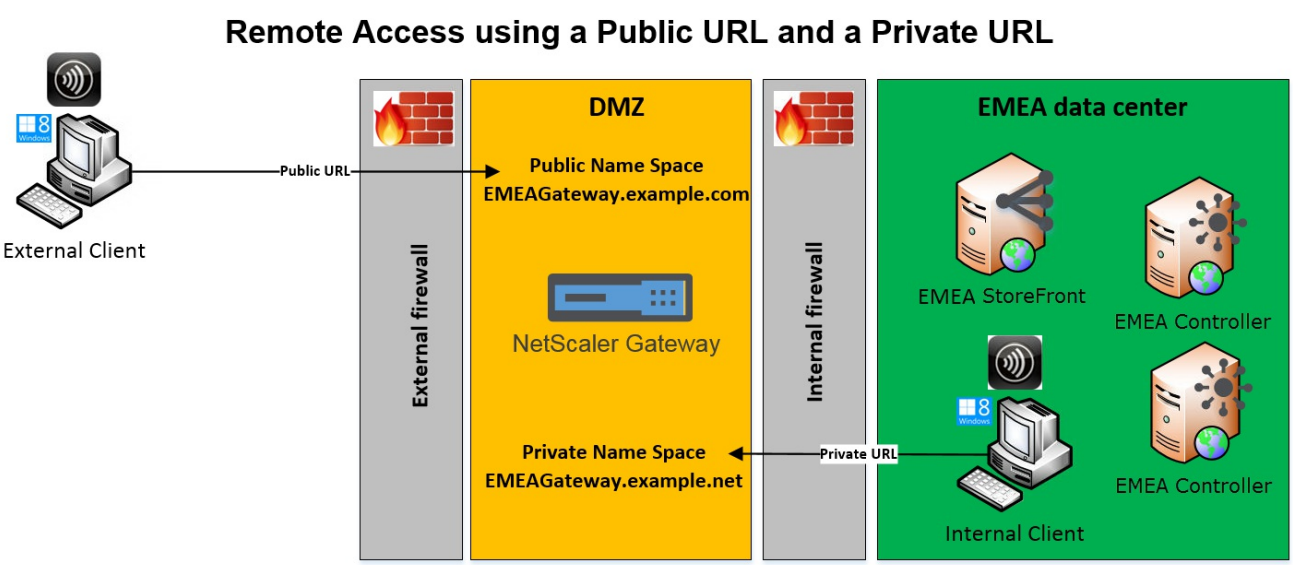


En este ejemplo:

- Cada ubicación o centro de datos contiene al menos una puerta de enlace, uno o varios servidores StoreFront y uno o varios Controllers de XenApp y XenDesktop para ofrecer recursos publicados en esa ubicación.
- Cada servicio GSLB configurado en los dispositivos NetScaler GSLB dentro de la implementación global representa un servidor virtual VPN de puerta de enlace. Todos los servidores StoreFront de la implementación deben estar configurados para que contengan todos los servidores virtuales de NetScaler Gateway que componen la capa de GSLB.
- Los NetScaler Gateway GSLB se usan en modo activo/activo pero también pueden usarse como alternativa de conmutación por error, para situaciones en que la conexión de red, el DNS, la puerta de enlace, el servidor StoreFront o los Controllers de XenApp y XenDesktop de una ubicación no respondan. Los usuarios se redirigen automáticamente a otra puerta de enlace si uno de los servicios GSLB no está disponible.
- Los clientes externos se dirigen a la puerta de enlace más cercana en función del algoritmo de equilibrio de carga GSLB que se haya configurado, tal como el tiempo de retorno (RTT) o la proximidad estática, cuando se establecen conexiones remotas.
- La dirección URL única para cada puerta de enlace permite a los usuarios seleccionar manualmente el centro de datos desde donde desean abrir recursos, eligiendo la URL específica de la ubicación de la puerta de enlace que quieran usar.
- El equilibrio de carga GSLB puede omitirse cuando GSLB o la delegación de DNS no funcione según lo previsto. Los usuarios pueden seguir accediendo los recursos remotos en cualquier centro de datos usando la URL específica de su ubicación, hasta que se resuelvan los problemas de GSLB.

Caso #2: NetScaler Gateway único con una URL pública o privada

El administrador usa el mismo NetScaler Gateway para el acceso externo (con una URL pública) y para el acceso interno (con una URL privada).



En este ejemplo:

- El administrador quiere que todo el acceso a los recursos publicados y el tráfico de HDX pasen a través de un NetScaler Gateway, incluso aunque el cliente sea interno.
- El NetScaler se encuentra en una zona desmilitarizada (DMZ).
- Existen dos rutas de red distintas al NetScaler Gateway a través de los dos firewalls situados a cada lado de la zona DMZ.
- El espacio de nombres externo, de cara al público, es distinto del espacio de nombres interno.

Ejemplos de cmdlets de PowerShell

Use los cmdlets de PowerShell **Add-STFRoamingGateway** y **Set-STFRoamingGateway** con el parámetro - gslburl, para establecer el atributo **GslbLocation** en el objeto de puerta de enlace de StoreFront. Por ejemplo:

comando COPIAR

```
Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com

Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://emeagateway.example.com" -GSLBurl "https://gslb.example.com

Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA gateway object)

Or

Get-STFRoamingGateway (returns all gateway object configured in StoreFront)
```

En caso de uso #1, puede quitar GSLBurl de "EMEAGateway" configurando su **GslbLocation** con el valor null. El siguiente comando de PowerShell modifica el objeto de la puerta de enlace $EMEAGateway almacenada en la memoria. **Set-STFRoamingGatway** puede recibir $EMEAGateway para actualizar la configuración de StoreFront y quitar GSLBurl.

comando COPIAR

```
$EMEAGateway = Get-STFRoamingGateway

$EMEAGateway.GslbLocation = $Null

Set-STFRoamingGateway -Gateway $EMEAGateway
```

En el caso #1, se devuelven las puertas de enlace siguientes al usar el comando **Get-STFRoamingGateway**:

comando COPIAR

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)

En el caso #2, se devuelven las puertas de enlace siguientes al usar el comando **Get-STFRoamingGateway**:

comando COPIAR

Name: **EMEAGateway**

Location: **https://emeagateway.example.com/** (Public URL for the Gateway)

GslbLocation: **https://emeagateway.example.net/** (Private URL for the Gateway)

En el caso #1, se devuelve el enrutamiento óptimo de puerta de enlace al usar el comando **Get-STFStoreRegisteredOptimalLaunchGateway**:

comando COPIAR

```
$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}**

La URL de GSLB o la URL interna para cada puerta de enlace se almacenan en el archivo web.config del servicio Roaming Service.

StoreFront no muestra la URL de GSLB o la dirección URL interna para cada puerta de enlace de NetScaler Gateway dentro de la consola de administración de StoreFront, pero es posible ver la ruta GSLBLocation configurada para todas las puertas de enlace GSLB, abriendo el archivo web.config del servicio Roaming Service en C:\inetpub\wwwroot\Citrix\Roaming\web.config en el servidor StoreFront.

Puertas de enlace del caso #1 en el archivo web.config del servicio Roaming

Puertas de enlace del caso #2 en el archivo web.config del servicio Roaming

Configuración de NetScaler y StoreFront para la autenticación con formularios delegada (DFA)

Aug 14, 2017

La autenticación extensible proporciona un único punto de personalización para la extensión de la autenticación con formularios de NetScaler y StoreFront. Para lograr una solución de autenticación mediante el SDK de autenticación extensible, debe configurar la autenticación con formularios delegada (DFA) entre NetScaler y StoreFront. El protocolo de autenticación con formularios delegada permite la generación y el procesamiento de formularios de autenticación, incluida la validación de credenciales, para que se deleguen a otro componente. Por ejemplo, NetScaler delega su autenticación a StoreFront, el cual interactúa con un servidor o servicio externo de autenticación.

Recomendaciones para la instalación

- Para garantizar que la comunicación entre NetScaler y StoreFront está protegida, utilice el protocolo HTTPS en lugar del protocolo HTTP.
- Para la implementación de clústeres, compruebe que todos los nodos tengan el mismo certificado de servidor instalado y configurado en el enlace HTTPS de IIS antes de proceder a la configuración.
- Compruebe que NetScaler tiene el emisor del certificado de servidor de StoreFront configurado como una entidad de certificación de confianza cuando HTTPS esté configurado en StoreFront.

Consideraciones acerca de la instalación de clústeres de StoreFront

- Instale un plug-in externo de autenticación en todos los nodos antes de unirlos.
- Configure todos los parámetros relacionados con la autenticación con formularios delegada en un nodo y propague los cambios a los demás. Consulte "Habilitación de la autenticación con formularios delegada".

Habilitación de la autenticación con formularios delegada

Como no hay ninguna interfaz gráfica de usuario para la configuración del parámetro de claves precompartidas de Citrix en StoreFront, utilice la consola de PowerShell para instalar la autenticación con formularios delegada.

1. Instale la autenticación con formularios delegada. No se instala de forma predeterminada, por lo que deberá instalarla mediante la consola de PowerShell.
   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
2. Agregue el Citrix Trusted Client. Configure la clave secreta compartida (frase de contraseña) entre StoreFront y NetScaler. La frase de contraseña y el ID del cliente deben ser idénticos a los que configuró en NetScaler.
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase secret
3. Establezca la Conversation Factory de la autenticación con formularios delegada para dirigir todo el tráfico al formulario personalizado. Para encontrar la Conversation Factory, busque ConversationFactory en C:\inetpub\wwwroot\Citrix\Authentication\web.config. He aquí un ejemplo de lo que puede ver.

4. En PowerShell, establezca la Conversation Factory de la autenticación con formularios delegada. En este ejemplo, para ExampleBridgeAuthentication.
   PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-DSDFAProperty -ConversationFactory ExampleBridgeAuthentication

Los argumentos de PowerShell no distinguen entre mayúsculas y minúsculas. Por ejemplo, -ConversationFactory es idéntico a -conversationfactory.

Desinstalación de StoreFront

Antes de desinstalar StoreFront, desinstale todos los plug-ins externos de autenticación, ya que afectará a la funcionalidad de StoreFront.

Autenticación con dominios distintos

Aug 14, 2017

Algunas organizaciones han establecido directivas que no permiten conceder a desarrolladores o contratistas externos el acceso a los recursos publicados en un entorno de producción. En este artículo se muestra cómo conceder acceso a los recursos publicados en un entorno de prueba. Para ello, los usuarios deberán autenticarse con un dominio a través de NetScaler Gateway. Luego, puede usar otro dominio para autenticarse en StoreFront y el sitio de Receiver para Web. La autenticación a través de NetScaler Gateway que se describe en este artículo se admite en caso de usuarios que inician sesión a través del sitio de Receiver para Web. Este método de autenticación no se admite en caso de usuarios de Citrix Receiver nativos móviles o de escritorio.

Configuración de un entorno de prueba

En este ejemplo se usa un dominio de producción llamado "production.com" y un dominio de prueba llamado "development.com".

Dominio production.com

Configuración del dominio "production.com" utilizado en este ejemplo:

- NetScaler Gateway con la directiva de autenticación LDAP configurada para "production.com".
- La autenticación a través de esa puerta de enlace se realiza con la cuenta y la contraseña production\testuser1.

Dominio development.com

Configuración del dominio "development.com" utilizado en este ejemplo:

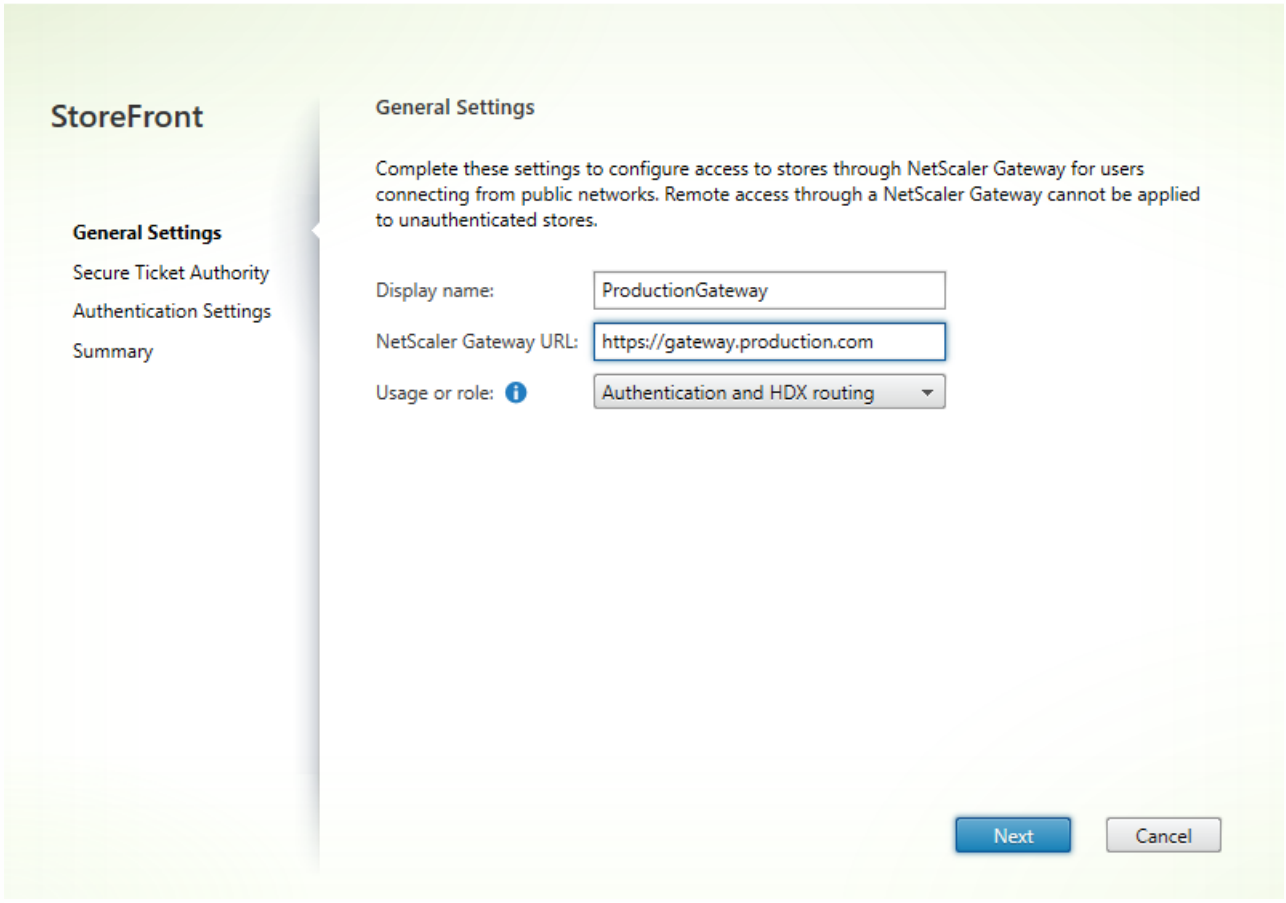
- StoreFront, XenApp y XenDesktop 7.0 o posterior y los VDA están en el dominio "development.com".
- La autenticación en el sitio Web de Citrix Receiver se produce con la cuenta y la contraseña development\testuser1.
- No hay ninguna relación de confianza entre los dos dominios.

Configuración de un NetScaler Gateway para la tienda

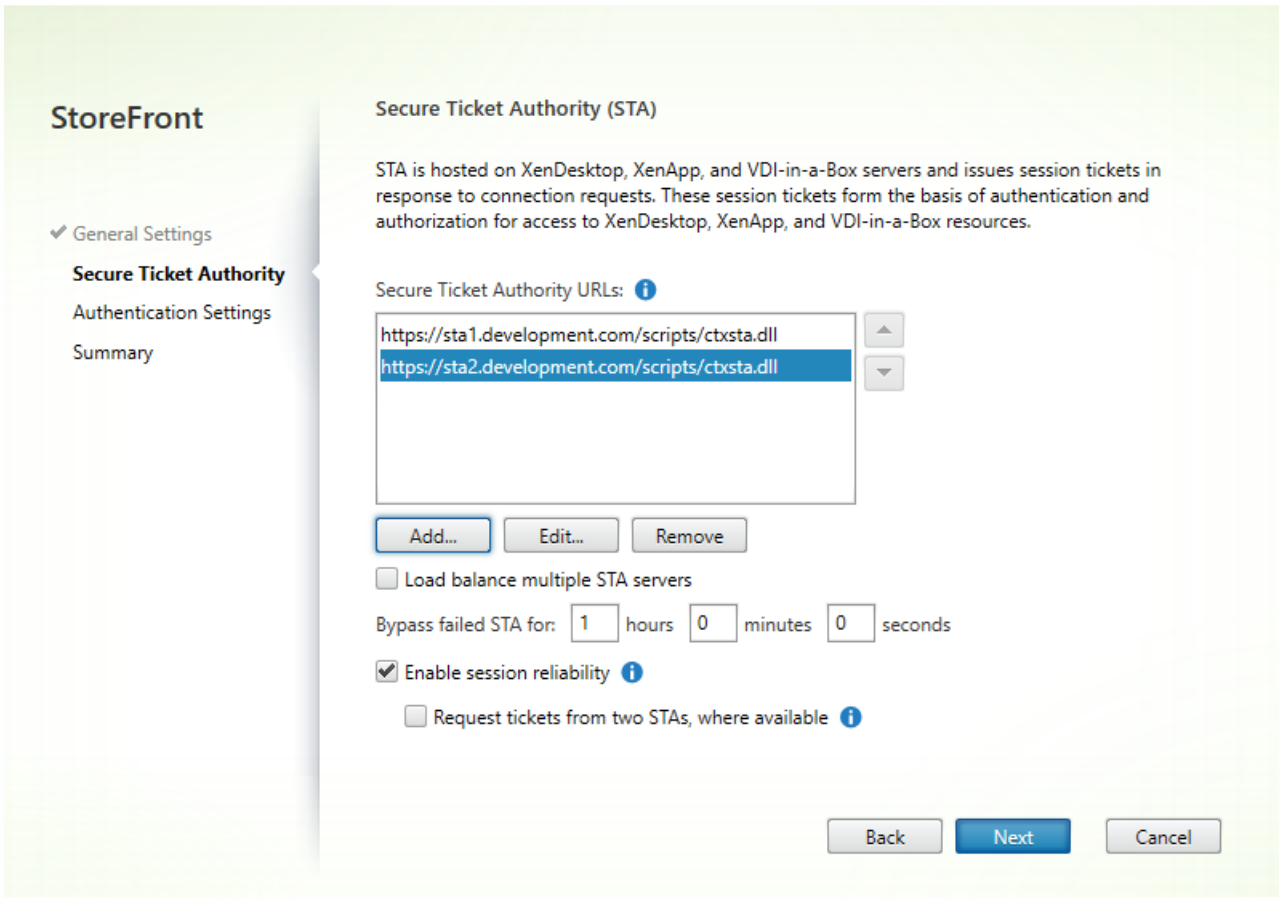
Para configurar un NetScaler Gateway para la tienda

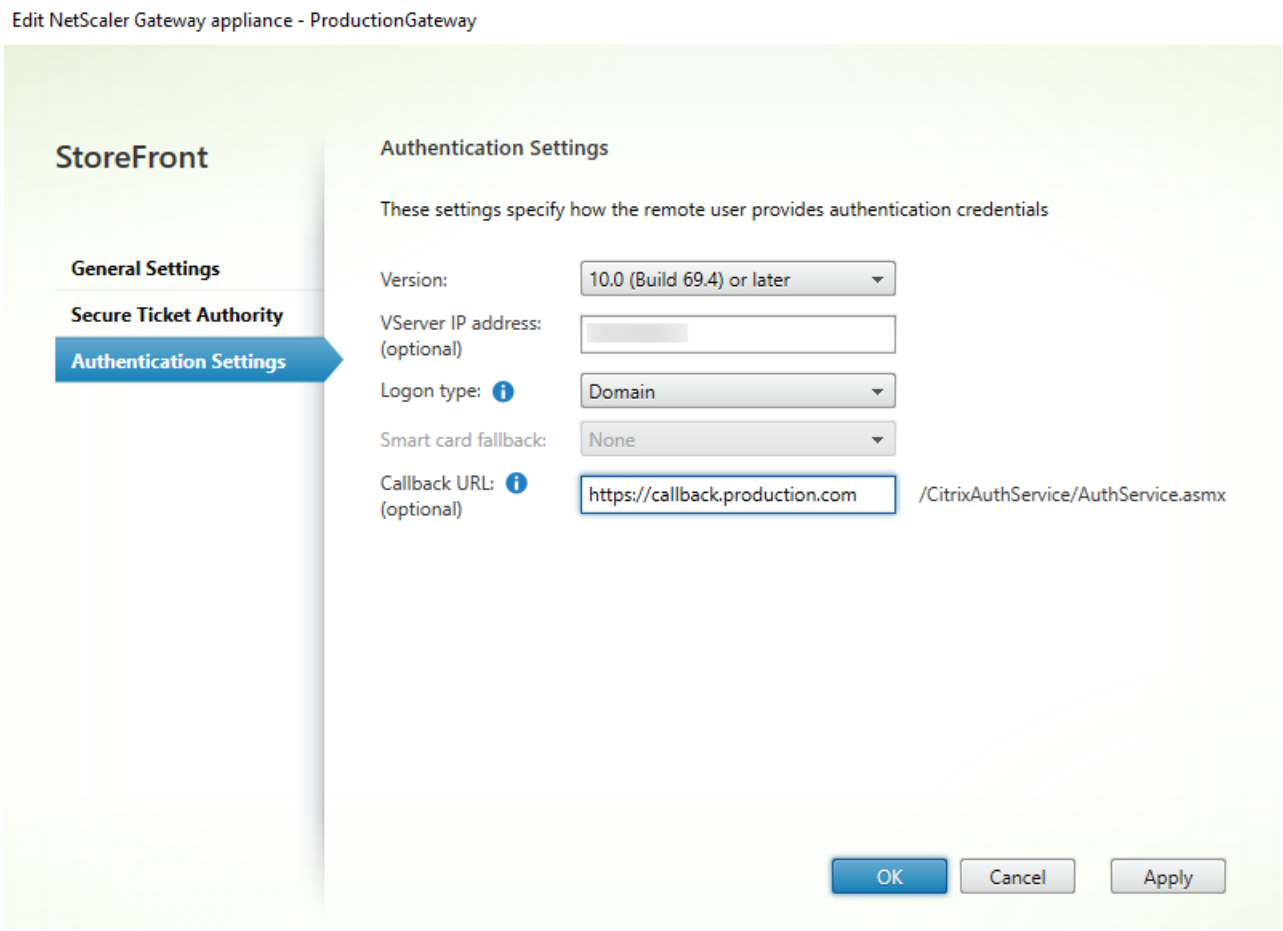
1. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones,** haga clic en **Administrar NetScaler Gateway**.
2. En la pantalla "Administrar NetScaler Gateway", haga clic en el botón **Agregar**.
3. Complete los pasos de Configuración general, de Secure Ticket Authority y de Autenticación.

Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance



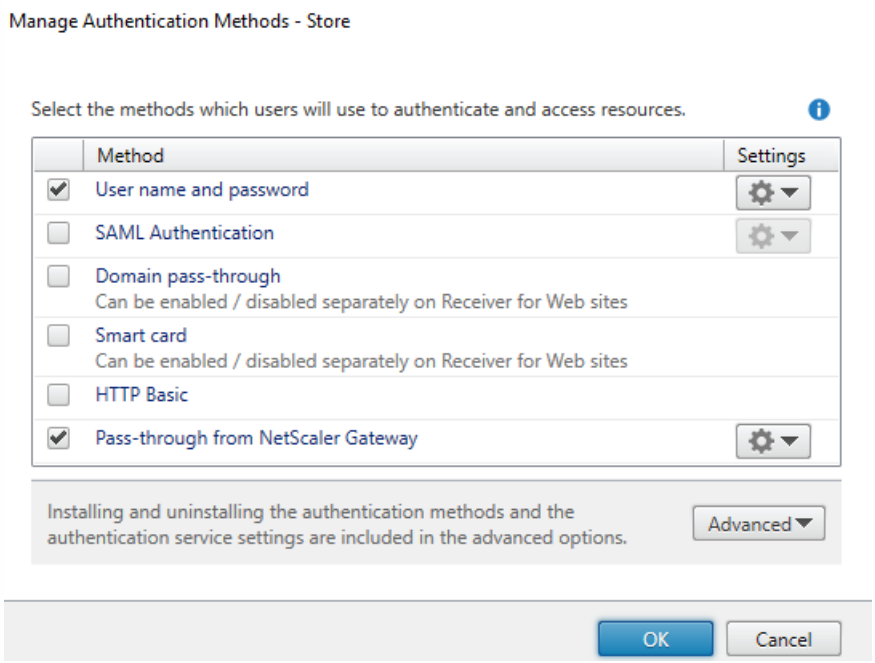


Nota

Puede que deba agregar reenviadores DNS condicionales para que los servidores DNS en ejecución en ambos dominios puedan resolver los FQDN en el otro dominio. NetScaler debe poder resolver los nombres FQDN del servidor STA en el dominio "development.com" con su servidor DNS de "production.com". StoreFront también debe poder resolver la URL de respuesta en el dominio "production.com" con su servidor DNS de "development.com". De forma alternativa, se puede utilizar un nombre FQDN de "development.com" que resuelva a la IP virtual (VIP) del servidor virtual de NetScaler Gateway.

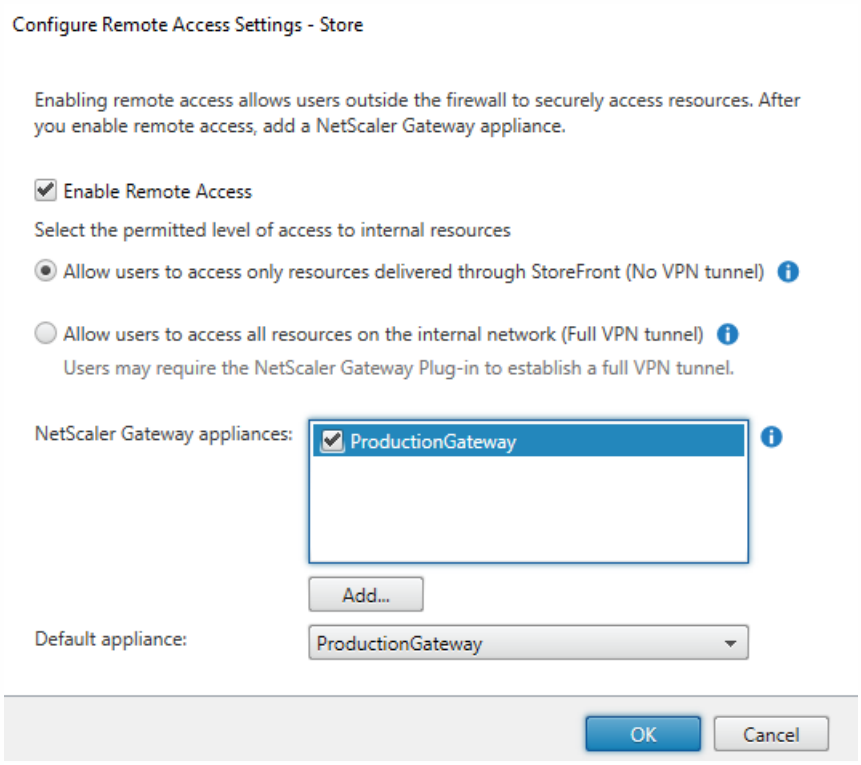
Cómo habilitar PassThrough desde NetScaler Gateway

1. Seleccione **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
2. En la pantalla "Administrar métodos de autenticación", seleccione **PassThrough desde NetScaler Gateway**.
3. Haga clic en **Aceptar**.



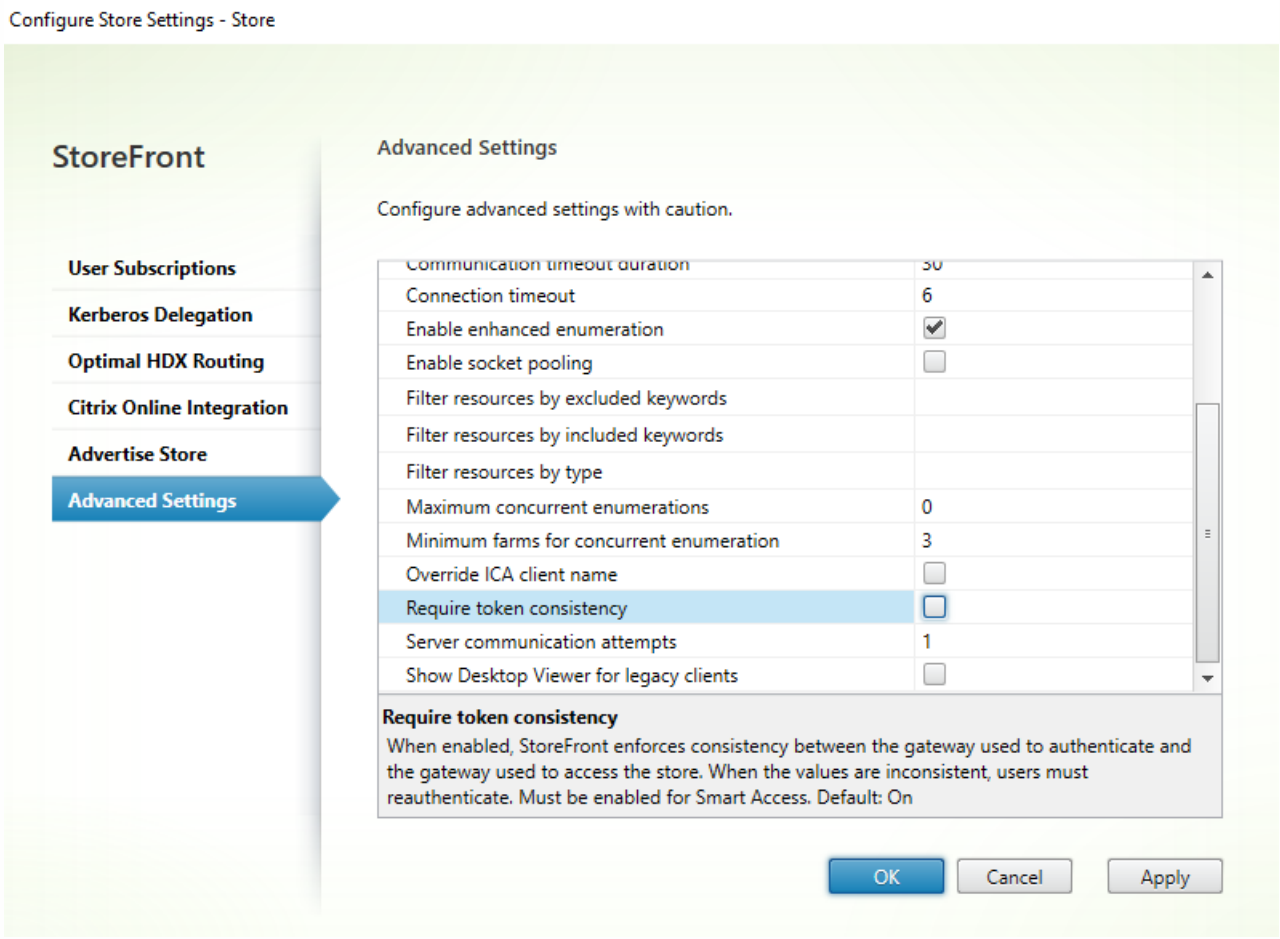
Configuración de la tienda para el acceso remoto a través de Gateway

1. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel **Acciones**, haga clic en **Configurar parámetros de acceso remoto**.
2. Seleccione **Habilitar acceso remoto**.
3. Compruebe que ha registrado el NetScaler Gateway en la tienda. Si no ha registrado el NetScaler Gateway, la generación de tíquets STA no funcionará.



Cómo inhabilitar la coherencia de tokens

1. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una tienda. En el panel **Acciones**, haga clic en **Configurar parámetros de la tienda**.
2. En la página "Configurar parámetros de la tienda", seleccione **Parámetros avanzados**.
3. Desmarque la casilla **Requerir coherencia de token**. Para obtener más información, consulte Parámetros avanzados de tiendas.
4. Haga clic en **Aceptar**.



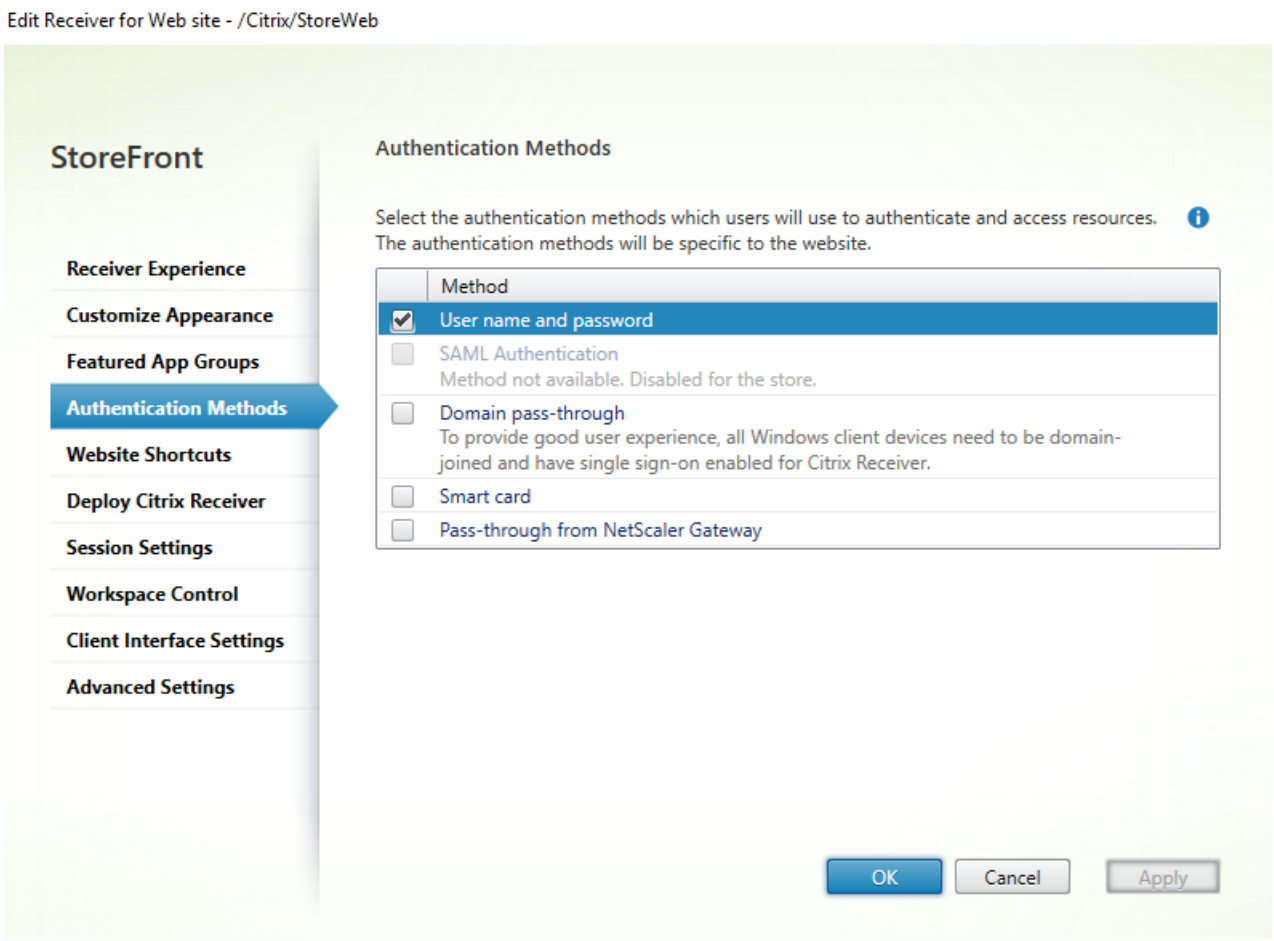
> ## Nota
>
> El parámetro "Requerir coherencia de token" está marcado (activado) de forma predeterminada. Si lo inhabilita, las funciones de SmartAccess utilizadas para NetScaler End Point Analysis (EPA) dejan de funcionar. Para obtener más información sobre SmartAccess, consulte CTX138110.

Cómo inhabilitar la autenticación PassThrough desde NetScaler Gateway para el sitio de Receiver para Web

> ## Important
>
> Inhabilitar la autenticación PassThrough desde NetScaler Gateway impide que Receiver para Web use las credenciales incorrectas

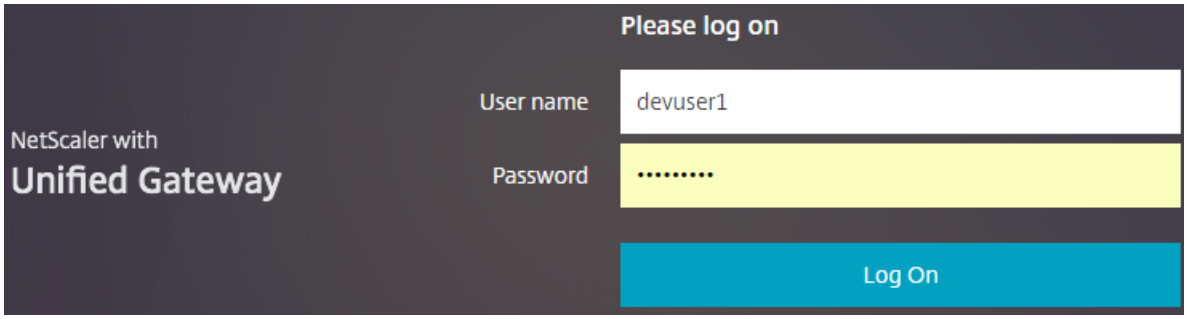
del dominio "production.com" transferido desde NetScaler. Inhabilitar la autenticación PassThrough desde NetScaler Gateway hace que Receiver para Web solicite al usuario que introduzca las credenciales. Estas no son las credenciales que se utilizan para iniciar sesión a través de Netscaler Gateway.

1. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront.
2. Seleccione la **tienda** que quiere modificar.
3. En el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web**.
4. En "Métodos de autenticación", desmarque la casilla "PassThrough desde NetScaler Gateway".
5. Haga clic en **Aceptar**.

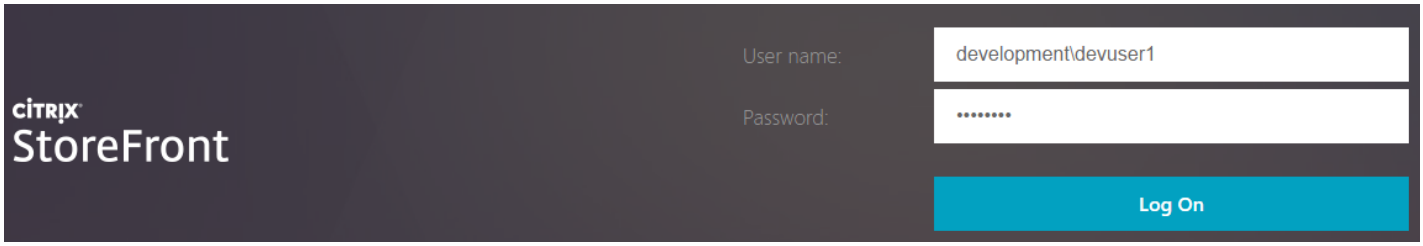


Inicio de sesión en Gateway con el usuario y las credenciales de "production.com"

Para realizar pruebas, inicie sesión en Gateway con un usuario y unas credenciales de "production.com".



Después de iniciar sesión, se le solicita que introduzca las credenciales de "development.com".

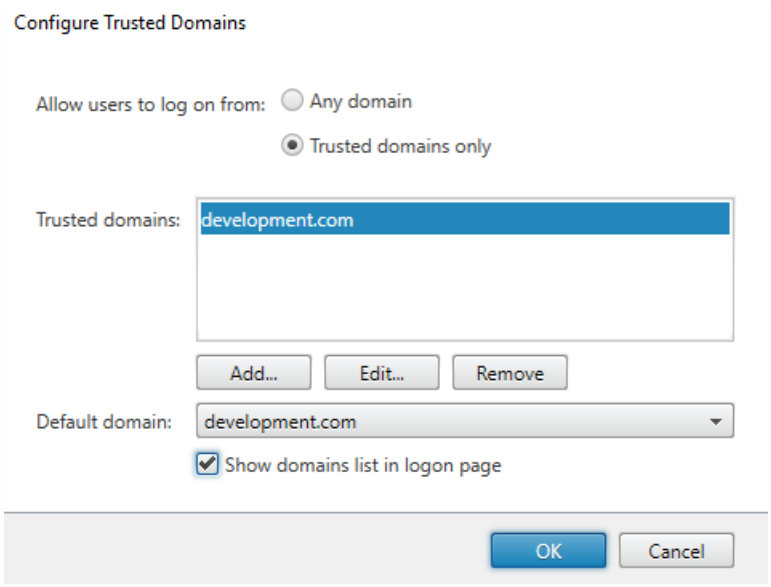


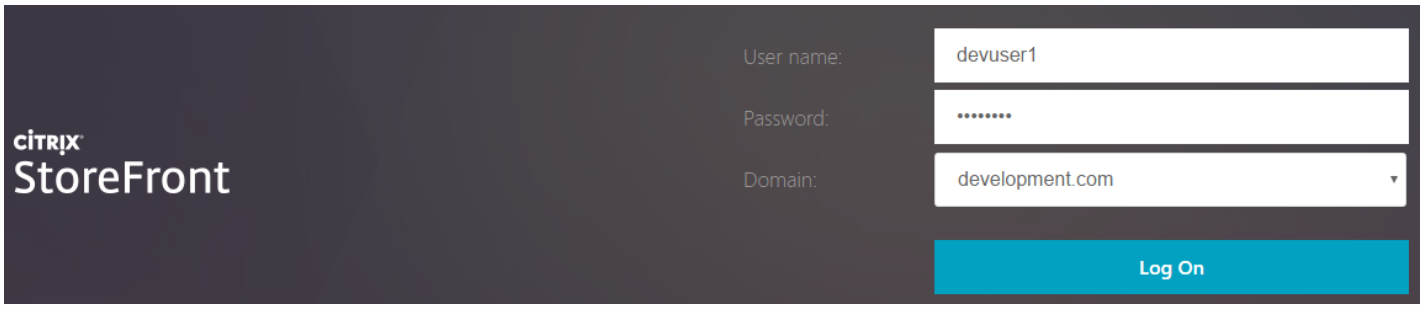
Cómo agregar una lista desplegable de dominios de confianza en StoreFront (opcional)

Este parámetro es optativo, pero puede contribuir a evitar que el usuario introduzca accidentalmente el dominio incorrecto para autenticarse a través de NetScaler Gateway.

Si el nombre de usuario es el mismo para ambos dominios, introducir el dominio incorrecto es más probable. También es posible que los usuarios nuevos tiendan a dejarse el dominio cuando inicien sesión a través de NetScaler Gateway. Entonces, podrían olvidarse de introducir el dominio y el nombre de usuario para el segundo dominio cuando se les pida iniciar sesión en el sitio de Receiver para Web.

1. Seleccione **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación**.
2. Seleccione la flecha desplegable ubicada junto a **Nombre de usuario y contraseña**.
3. Haga clic en **Agregar** para agregar "development.com" como dominio de confianza y marque la casilla **Mostrar lista de dominios en la página de inicio de sesión**.
4. Haga clic en **Aceptar**.



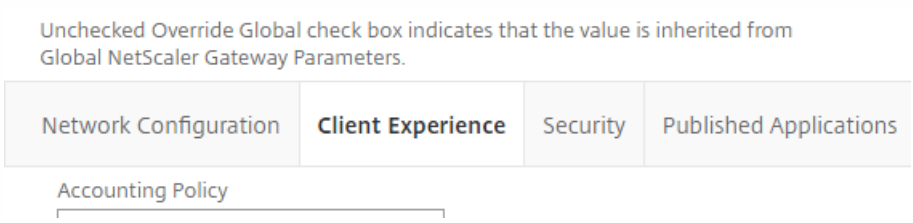


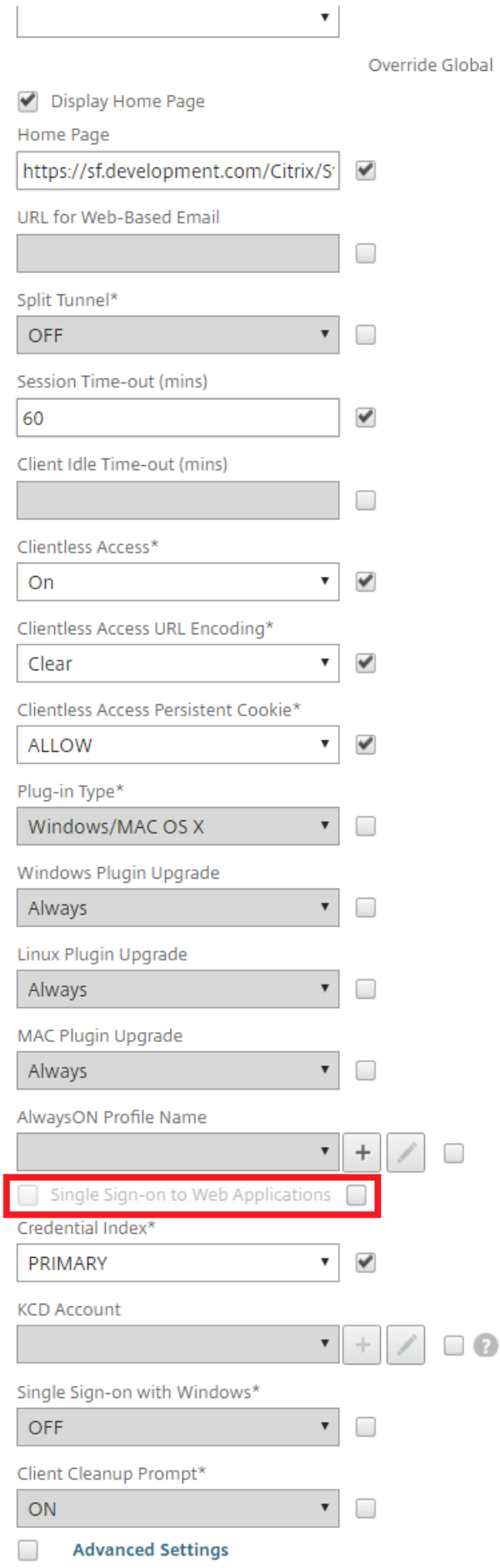
Nota

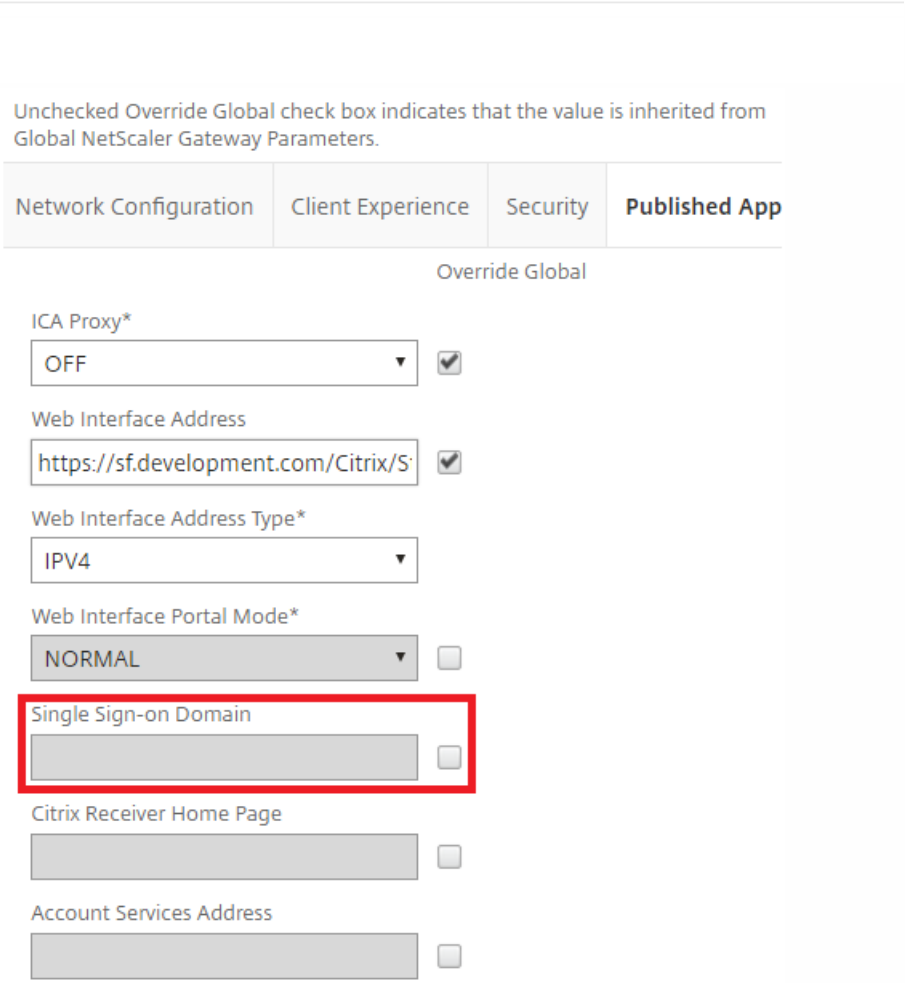
En este caso de autenticación, no se recomienda que el explorador Web tenga habilitado el almacenamiento en caché de las contraseñas. Si los usuarios tienen contraseñas diferentes para las dos cuentas de dominios distintos, el almacenamiento en caché de las contraseñas puede dar lugar a una mala experiencia de usuario.

Directiva de acción en la sesión de VPN (CVPN) sin cliente de NetScaler

- Si se habilita el inicio Single Sign-On a las aplicaciones Web en la directiva de sesiones NetScaler, las credenciales incorrectas que envíe NetScaler a Receiver para Web se ignoran porque se ha inhabilitado el método de autenticación **PassThrough desde NetScaler Gateway** en el sitio de Receiver para Web. Receiver para Web solicita credenciales independientemente de esta opción.
- Completar los datos de las entradas Single Sign-On en las fichas de experiencia de cliente y de aplicación publicada en NetScaler no modifica el comportamiento que se describe en este artículo.







Configuración de balizas

Aug 14, 2017

Utilice la tarea Administrar balizas y especifique las direcciones URL para utilizarlas como balizas. Estas URL pueden pertenecer tanto a la red interna como a la externa. Citrix Receiver intenta comunicarse con las balizas y usa las respuestas para determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un escritorio o aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan devolver a Citrix Receiver los correspondientes datos de conexión. Esto garantiza que a los usuarios no se les solicitará que inicien sesión de nuevo cuando accedan a un escritorio o aplicación.

Por ejemplo: si la baliza interna es accesible, esto indica que el usuario está conectado a la red local. Sin embargo, si Citrix Receiver no puede ponerse en contacto con la baliza interna y recibe respuestas de las dos balizas externas, esto significa que el usuario tiene una conexión a Internet, pero está fuera de la red corporativa. Por tanto, el usuario debe conectarse a los escritorios y aplicaciones a través de NetScaler Gateway. Cuando un usuario accede a un escritorio o aplicación, se notifica al servidor que proporciona el recurso para que proporcione la información del dispositivo NetScaler Gateway a través del que debe enrutarse la conexión. Esto significa que el usuario no necesita iniciar sesión en el dispositivo para acceder al escritorio o a la aplicación.

De forma predeterminada, StoreFront utiliza la dirección URL del servidor o la dirección URL con equilibrio de carga de la implementación como baliza interna. El sitio Web de Citrix y la URL del servidor virtual o punto de entrada (para Access Gateway 5.0) de la primera implementación de NetScaler Gateway que usted agrega se utilizan como balizas externas de forma predeterminada.

Si cambia una baliza, asegúrese de que los usuarios actualicen Citrix Receiver con la información actualizada. Cuando un sitio de Receiver para Web está configurado para una tienda, los usuarios pueden obtener un archivo de aprovisionamiento de Citrix Receiver actualizado desde el sitio. De lo contrario, puede exportar un archivo de aprovisionamiento para la tienda y poner este archivo a disposición de los usuarios.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Tiendas** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en Administrar balizas.
3. Especifique la dirección URL que se va a usar como baliza interna.
   - Para usar la URL del servidor o la URL de equilibrio de carga de la implementación de StoreFront, seleccione Usar URL de servicio.
   - Para usar una URL alternativa, seleccione Especificar dirección de baliza y escriba una URL de alta disponibilidad que forme parte de la red interna.
4. Haga clic en Agregar para especificar la URL de una baliza externa. Para modificar una baliza, seleccione la URL de la lista Balizas externas y haga clic en Modificar. Seleccione una URL de la lista y haga clic en Quitar para dejar de utilizar esa dirección como baliza.
   Debe especificar al menos dos balizas externas de alta disponibilidad que se pueden resolver desde redes públicas. Las direcciones URL de balizas deben ser nombres de dominio completos (por ejemplo: http://ejemplo.com), no el nombre abreviado NetBIOS (http://ejemplo). Esto permite que Citrix Receiver determine si los usuarios se encuentran en redes de Internet de pago, como las de un hotel o una cafetería con servicio de Internet. En tales casos, todas las balizas externas

se conectan al mismo proxy.

Configuraciones avanzadas

Aug 14, 2017

StoreFront ofrece opciones avanzadas que se pueden configurar mediante la consola de StoreFront, PowerShell, propiedades de certificado o archivos de configuración.

Configuración de los sitios de Desktop Appliance	Puede crear, eliminar y modificar sitios de Desktop Appliance.
Creación de un nombre de dominio completo (FQDN) para acceder a una tienda de forma interna y externa	Puede proporcionar acceso a los recursos desde la red corporativa o desde Internet a través de NetScaler Gateway y simplificar la experiencia de los usuarios mediante la creación de un único nombre de dominio completo para clientes internos y clientes externos móviles.
Configuración del filtro de recursos	Puede filtrar recursos de enumeración según el tipo de recurso y las palabras clave.

Configuración de los sitios de Desktop Appliance

Aug 14, 2017

A continuación se describe cómo crear, quitar y modificar sitios de Desktop Appliance. Para crear o quitar sitios, debe ejecutar comandos de Windows PowerShell. Los cambios en la configuración de un sitio de Desktop Appliance se realizan editando los archivos de configuración del sitio.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.
Nota: Las consolas de StoreFront y PowerShell no pueden estar abiertas al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.

Para crear o quitar sitios de Desktop Appliance

Solo se puede acceder a un único almacén a través de cada sitio de Desktop Appliance. Puede crear un almacén que contenga todos los recursos que desea poner a disposición de los usuarios que tengan dispositivos de escritorio no unidos a un dominio. De forma alternativa, puede crear almacenes independientes, cada uno con un sitio de Desktop Appliance, y configurar los dispositivos de escritorio de los usuarios para conectar con el sitio correspondiente.

1. Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell y, en el símbolo del sistema, escriba el siguiente comando para importar los módulos de StoreFront.
   & "installationlocation\Scripts\ImportModules.ps1"
   Donde installationlocation es el directorio en el que StoreFront está instalado, normalmente C:\Archivos de programa\Citrix\Receiver StoreFront\.

2. Para crear un nuevo sitio de Desktop Appliance, escriba el siguiente comando.
   Install-DSDesktopAppliance -FriendlyName sitename -SiteId iisid -VirtualPath sitepath -UseHttps {$False | $True} -StoreUrl storeaddress [-EnableMultiDesktop {$False | $True}] [-EnableExplicit {$True
   Donde sitename es el un nombre que le ayude a identificar el sitio de Desktop Appliance. Para iisid, especifique el ID numérico del sitio de Microsoft Internet Information Services (IIS) que aloja StoreFront, que se puede obtener de la consola del administrador de Internet Information Services (IIS). Reemplace sitepath por la ruta relativa donde se debe crear el sitio en IIS, por ejemplo: /Citrix/DesktopAppliance. Tenga en cuenta que las direcciones URL de los sitios de Desktop Appliance distinguen entre mayúsculas y minúsculas.

   Indique si StoreFront está configurado para HTTPS estableciendo -UseHttps en el valor apropiado.

   Para especificar la URL absoluta del servicio de tienda usado porel sitio de Desktop Appliance Connector, use StoreUrl storeaddress. Este valor se muestra en el resumen de almacén en la consola de administración.

   De forma predeterminada, cuando un usuario inicia sesión en un sitio de Desktop Appliance, el primer escritorio disponible para el usuario se inicia automáticamente. Para configurar el nuevo sitio de Desktop Appliance para que los usuarios puedan elegir entre varios escritorios, si están disponibles, establezca -EnableMultiDesktop en $True.

   La autenticación explícita está habilitada de forma predeterminada para los nuevos sitios. Puede inhabilitar la autenticación explícita estableciendo el argumento -EnableExplicit en $False. Habilite la autenticación con tarjeta inteligente estableciendo -EnableSmartCard en $True. Para habilitar la autenticación PassThrough con tarjeta inteligente, debe establecer -EnableSmartCard y -EnableEmbeddedSmartCardSSO en $True. Si habilita la autenticación explícita, además de la autenticación con tarjeta inteligente o la autenticación PassThrough con tarjeta inteligente, a los usuarios se les solicita inicialmente que inicien sesión con una tarjeta inteligente, pero pueden recurrir a la autenticación explícita si los usuarios tienen problemas con las tarjetas inteligentes.

   Los argumentos optativos configuran parámetros que también se pueden modificar después de que el sitio de Desktop Appliance se haya creado mediante la edición del archivo de configuración del sitio.

   Ejemplo:

   Crear un sitio de Desktop Appliance Connector en la ruta virtual /Citrix/DesktopAppliance1 en el sitio Web IIS predeterminado.

   Install-DSDesktopAppliance `

   -FriendlyName DesktopAppliance1 `

   -SiteId 1 `

   -VirtualPath /Citrix/DesktopAppliance1 `

   -UseHttps $false `

   -StoreUrl https://nombreDelServidor/Citrix/Store `

   -EnableMultiDesktop $true `

   -EnableExplicit $true `

   -EnableSmartCard $true `

   -EnableEmbeddedSmartCardSSO $false

3. Para quitar un sitio de Desktop Appliance existente, escriba el siguiente comando.
   Remove-DSDesktopAppliance -SiteId iisid -VirtualPath sitepath
   Donde iisid es el ID numérico del sitio de IIS que aloja StoreFront y sitepath es la ruta relativa del sitio de Desktop Appliance en IIS, por ejemplo: /Citrix/DesktopAppliance.

4. Para ver una lista de los sitios de Desktop Appliance actualmente disponibles desde su implementación de StoreFront, escriba el siguiente comando.
   Get-DSDesktopAppliancesSummary

Para configurar la autenticación de usuario

Los sitios de Desktop Appliance admiten la autenticación explícita, la autenticación con tarjeta inteligente y la autenticación PassThrough con tarjeta inteligente. La autenticación explícita está habilitada de forma predeterminada. Si habilita la autenticación explícita, además de la autenticación con tarjeta inteligente o la autenticación PassThrough con tarjeta inteligente, el comportamiento predeterminado inicialmente solicita a los usuarios que inicien sesión con una tarjeta inteligente. A los usuarios que experimenten problemas con sus tarjetas inteligentes se les da la opción de escribir credenciales explícitas. Si configura IIS para requerir certificados de cliente en conexiones HTTPS para todas las direcciones URL de StoreFront, los usuarios no pueden recurrir a la autenticación explícita cuando no pueden utilizar las tarjetas inteligentes. Para configurar los métodos de autenticación de un sitio de Desktop Appliance, edite el archivo de configuración del sitio.

1. Utilice un editor de texto para abrir el archivo web.config para el sitio de Desktop Appliance, que normalmente se encuentra en el directorio

C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance, donde storename es el nombre especificado para la tienda durante su creación.
2. Localice el siguiente elemento en el archivo.
3. Cambie el valor del atributo enabled a false para inhabilitar la autenticación explícita para el sitio.
4. Locate the following element in the file.

5. Establezca el valor del atributo enabled en true para habilitar la autenticación con tarjeta inteligente. Para habilitar la autenticación PassThrough con tarjeta inteligente, también debe establecer el valor del atributo useEmbeddedSmartcardSso en true. Utilice el atributo embeddedSmartcardSsoPinTimeout para establecer el tiempo (en horas, minutos y segundos) que se muestra la pantalla de entrada del PIN antes de agotar el tiempo de espera. Cuando se agota el tiempo de espera de la pantalla de entrada del PIN, los usuarios vuelven a la pantalla de inicio de sesión y deben quitar y volver a insertar la tarjeta inteligente para obtener acceso a la pantalla de entrada del PIN de nuevo. El período de tiempo de espera se establece en 20 segundos de forma predeterminada.

Para permitir que los usuarios puedan elegir entre varios escritorios

De forma predeterminada, cuando un usuario inicia sesión en un sitio de Desktop Appliance, se inicia automáticamente el primer escritorio (en orden alfabético) disponible para el usuario en el almacén para el que se ha configurado el sitio. Si proporciona a los usuarios acceso a varios escritorios de una tienda, puede configurar el sitio de Desktop Appliance para que muestre todos los escritorios disponibles. De esta manera, los usuarios pueden elegir el escritorio al que acceder. Para cambiar estos parámetros, edite el archivo de configuración del sitio.

1. Utilice un editor de texto para abrir el archivo web.config para el sitio de Desktop Appliance, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storenameDesktopAppliance, donde storename es el nombre especificado para la tienda durante su creación.
2. Localice el siguiente elemento en el archivo.
3. Cambie el valor del atributo showMultiDesktop a true para permitir que los usuarios vean y seleccionen entre todos los escritorios disponibles para ellos en la tienda cuando inician sesión en el sitio de Desktop Appliance.

Creación de un nombre de dominio completo (FQDN) para acceder a una tienda de forma interna y externa

Aug 14, 2017

Nota: Para usar esta característica con Receivers nativos de escritorio, se necesitan las versiones siguientes.

- Receiver para Windows 4.2
- Receiver para Mac 11.9

Puede proporcionar acceso a los recursos desde la red corporativa o desde Internet a través de NetScaler Gateway y simplificar la experiencia de los usuarios mediante la creación de un único nombre de dominio completo para clientes internos y clientes externos móviles.

La creación de un único nombre de dominio completo es útil para los usuarios que configuren cualquiera de los Receiver nativos. Solo necesitan recordar una sola dirección URL y si se han conectado a una red interna o a una red pública.

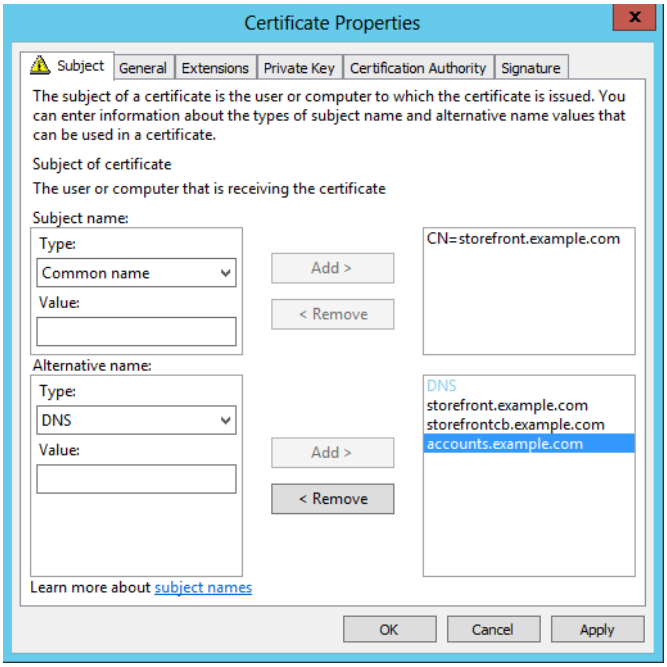
Balizas de StoreFront para Receivers nativos

Citrix Receiver intenta comunicarse con las balizas y usa las respuestas para determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un escritorio o aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan devolver a Citrix Receiver los correspondientes datos de conexión. Esto garantiza que a los usuarios no se les solicitará que inicien sesión de nuevo cuando accedan a un escritorio o aplicación. Para obtener información sobre la configuración de balizas, consulte Configuración de balizas.

Configuración del certificado de SSL y del servidor virtual de NetScaler Gateway

El nombre de dominio completo se resuelve en la dirección IP del enrutador de un firewall externo o en la dirección IP del servidor virtual de NetScaler Gateway de la zona desmilitarizada (DMZ) cuando los clientes externos intentan acceder a recursos desde fuera de la red corporativa. Compruebe que los campos Nombre común y Nombre alternativo del firmante del certificado SSL contengan el nombre de dominio completo compartido que se utilizará para acceder a la tienda de forma externa. Al emplear una entidad de certificación (CA) raíz externa como VeriSign en lugar de una entidad de certificación empresarial para firmar el certificado de la puerta de enlace, cualquier cliente externo confía automáticamente en el certificado enlazado al servidor virtual de puerta de enlace. Si emplea una CA raíz externa como VeriSign, no se necesita importar más certificados de CA raíz en los clientes externos.

Para implementar un único certificado con el nombre común del nombre de dominio completo compartido en NetScaler Gateway y en el servidor StoreFront, tenga en cuenta si quiere que respalden la detección remota. Si es que sí, compruebe que el certificado cumple con las especificaciones de los nombres alternativos del firmante.



Certificado de ejemplo de un servidor virtual de NetScaler Gateway: storefront.example.com

1. Compruebe que el nombre de dominio completo compartido, la URL de respuesta y la URL de alias de cuenta se incluyen en el campo DNS como nombre alternativo del sujeto (SAN - Subject Alternative Name).
2. Compruebe también que la clave privada se puede exportar para que el certificado y la clave se puedan importar en NetScaler Gateway.
3. Asegúrese de que Autorización predeterminada tenga el valor Permitir.
4. Firme el certificado mediante una entidad de certificación externa como VeriSign o mediante una entidad de certificación empresarial de la organización.

Ejemplos de nombres SAN de grupos de servidores de dos nodos:

storefront.ejemplo.com (obligatorio)

storefrontcb.ejemplo.com (obligatorio)

cuentas.ejemplo.example.com (obligatorio)

storefrontserver1.ejemplo.com (optativo)

storefrontserver2.ejemplo.com (optativo)

Firma del certificado SSL del servidor virtual de NetScaler Gateway con una entidad de certificación (CA)

Según sus requisitos, tiene dos opciones para elegir el tipo de certificado firmado por una entidad de certificación.

- Opción 1: Certificado firmado por una entidad de certificación externa. Si el certificado enlazado al servidor virtual de NetScaler Gateway está firmado por una entidad externa de confianza, es muy posible que los clientes externos NO necesiten copiar certificados de CA raíz en sus almacenes de certificados de CA raíz de confianza. Los clientes de Windows se incluyen en los certificados de CA raíz de las agencias de firma más comunes. Se pueden emplear entidades externas y comerciales de certificación como DigiCert, Thawte y Verisign. Tenga en cuenta que los dispositivos móviles como iPhones, iPads y los teléfonos y las tabletas Android aún podrían requerir que la entidad de certificación raíz se copie al dispositivo para confiar en el servidor virtual de NetScaler Gateway.

- Opción 2: Certificado firmado por una CA raíz empresarial. Si elige esta opción, todos los clientes externos requieren que el certificado de CA raíz empresarial se copie en sus almacenes de certificados de CA raíz de confianza. Si se usan dispositivos portátiles con un Receiver nativo instalado, como un iPhone o un iPad, cree un perfil de seguridad en dichos dispositivos.

Importación del certificado raíz en dispositivos portátiles

- Los dispositivos iOS pueden importar archivos de certificado X.509 .CER mediante datos adjuntos de correo electrónico porque normalmente no se puede acceder al almacenamiento local de los dispositivos iOS.
- Los dispositivos Android también necesitan el formato X.509 .CER. El certificado se puede importar desde el almacenamiento local del dispositivo o desde los datos adjuntos de un correo electrónico.

DNS externo: storefront.example.com

Compruebe que la resolución de DNS proporcionada por el proveedor de servicios de Internet de la organización se resuelve en la dirección IP del enrutador del firewall que apunta al exterior en el borde exterior de la DMZ o a la dirección IP virtual del servidor virtual de NetScaler Gateway.

DNS partido

- Cuando el DNS partido (Split-view DNS) se configura correctamente, la dirección de origen de la solicitud DNS debe enviar el cliente al registro A de DNS correcto.
- Cuando los clientes se mueven entre redes públicas y empresariales, sus direcciones IP deben cambiar. Dependiendo de la red a la que estén conectados en ese momento, deben recibir el registro A correcto cuando hacen una consulta a storefront.ejemplo.com.

Importación de certificados emitidos por una entidad de certificación de Windows en NetScaler Gateway

WinSCP es una herramienta externa útil y gratuita para trasladar archivos de una máquina con Windows a un sistema de archivos de NetScaler Gateway. Copie los certificados que quiere importar en la carpeta /nsconfig/ssl/ del sistema de archivos de NetScaler Gateway. Puede usar las herramientas de OpenSSL en NetScaler Gateway para extraer el certificado y la clave de un archivo PKCS12/PFX y, así, crear dos archivos X.509 .CER y .KEY independientes en formato PEM que puede utilizar NetScaler Gateway.

1. Copie el archivo PFX en/nsconfig/ssl, en el dispositivo o el VPX de NetScaler Gateway.
2. Abra la interfaz de línea de comandos de NetScaler Gateway.
3. Para cambiar al shell de FreeBSD, escriba Shell para salir de la interfaz de línea de comandos de NetScaler Gateway.
4. Para cambiar el directorio, use cd /nsconfig/ssl.
5. Ejecute openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer e introduzca la contraseña de PFX cuando la pida el sistema.
6. Ejecute openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key
7. Escriba la contraseña del archivo PFX cuando se le solicite y, a continuación, establezca una frase de contraseña con formato PEM de clave privada para proteger el archivo KEY.
8. Para comprobar que los archivos CER y KEY se han creado correctamente en /nsconfig/ssl/, ejecute ls –al.
9. Para volver a la interfaz de línea de comandos de NetScaler Gateway, escriba Exit.

Directiva de sesiones de puerta de enlace de Receiver para Mac/Windows nativo

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

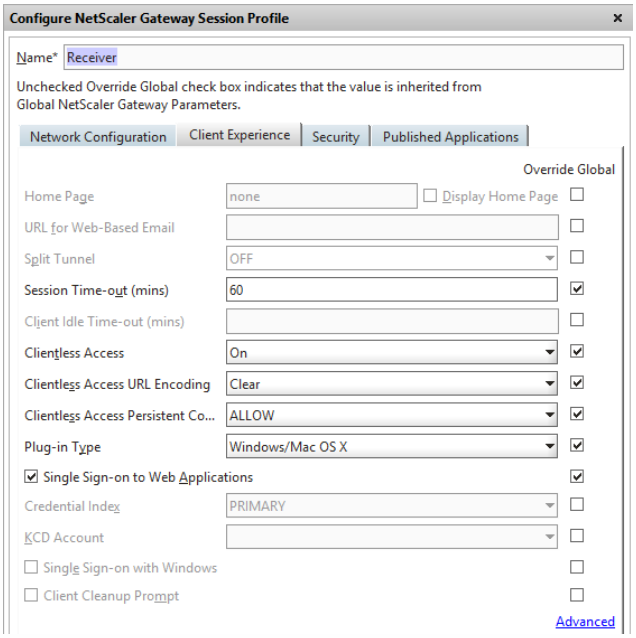
Directiva de sesiones de puerta de enlace de Receiver para Web

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

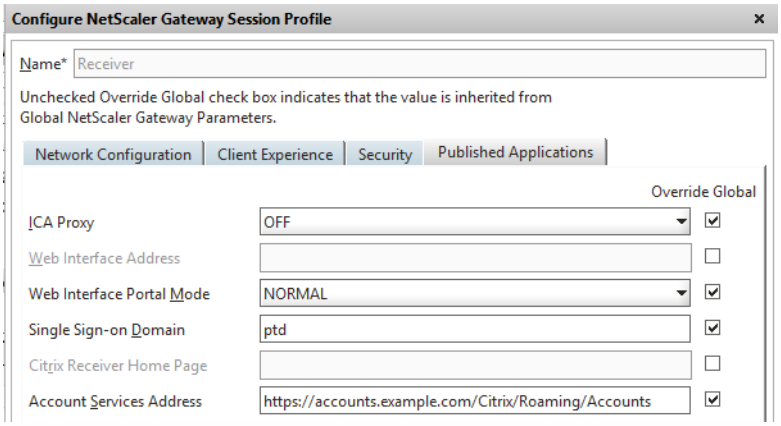
Parámetros de cVPN y Smart Access

Si usa el modo de acceso inteligente (Smart Access), habilítelo en la página de propiedades del servidor virtual de NetScaler Gateway. Se necesitan licencias universales para cada usuario concurrente o simultáneo que accede a recursos remotos.

Perfil de Receiver

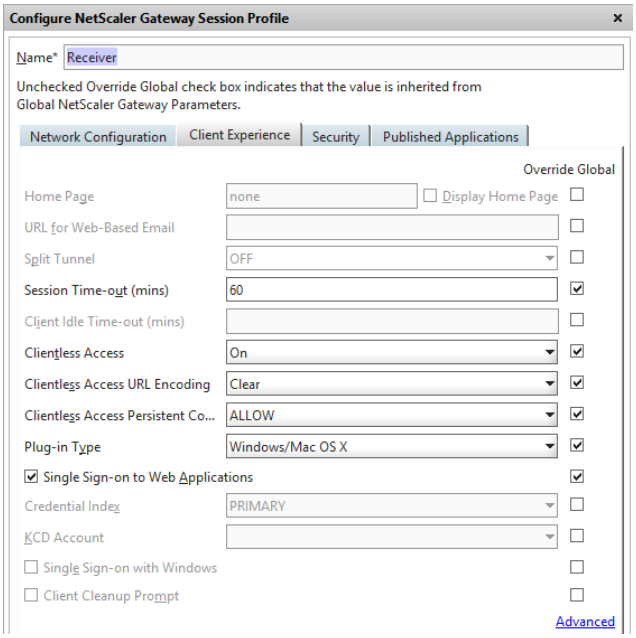


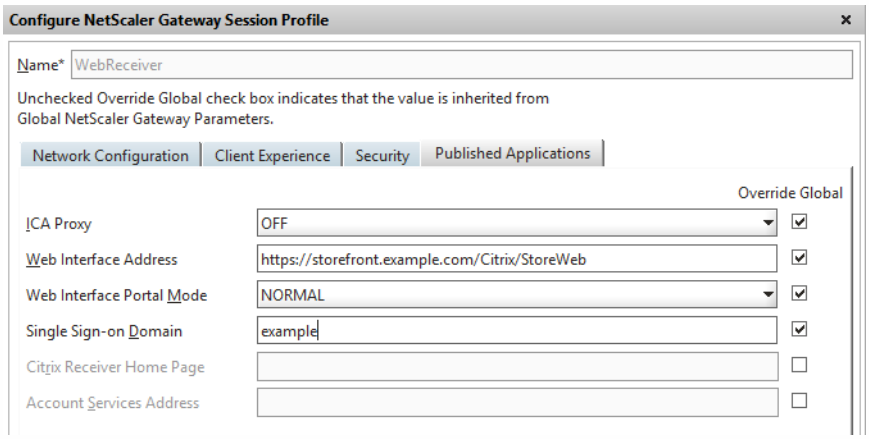
Configure la URL del servicio de cuentas de perfil de la sesión para que sea https://cuentas.ejemplo.com/Citrix/Roaming/Accounts y NO https://storefront.ejemplo.com/Citrix/Roaming/Accounts.



Agregue también esta URL como <allowedAudiences> adicional en los archivos web.config de los servicios de autenticación y Roaming en el servidor StoreFront. Para obtener más información, consulte "Configuración de la URL base del host, la puerta de enlace y el certificado SSL de un servidor StoreFront" en el apartado siguiente.

Perfil de Receiver para Web

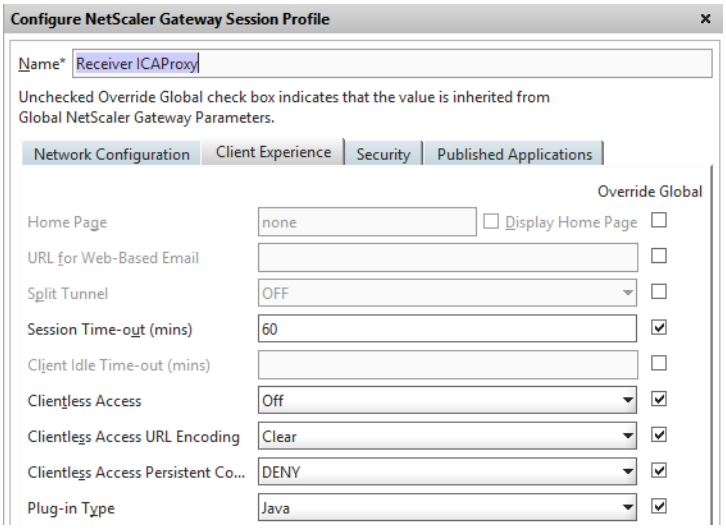


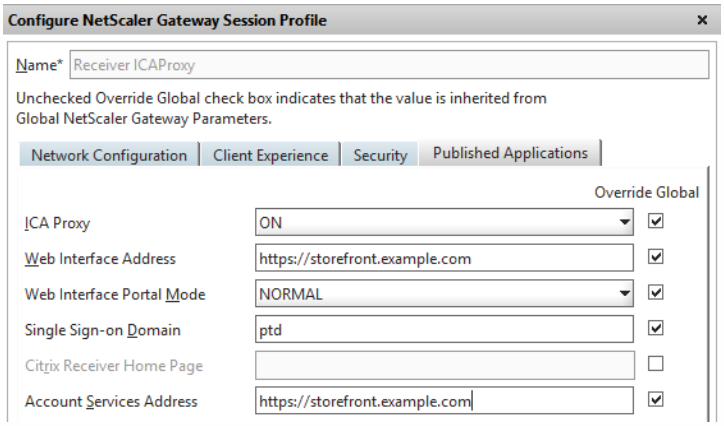


Parámetros de proxy ICA y modo Básico

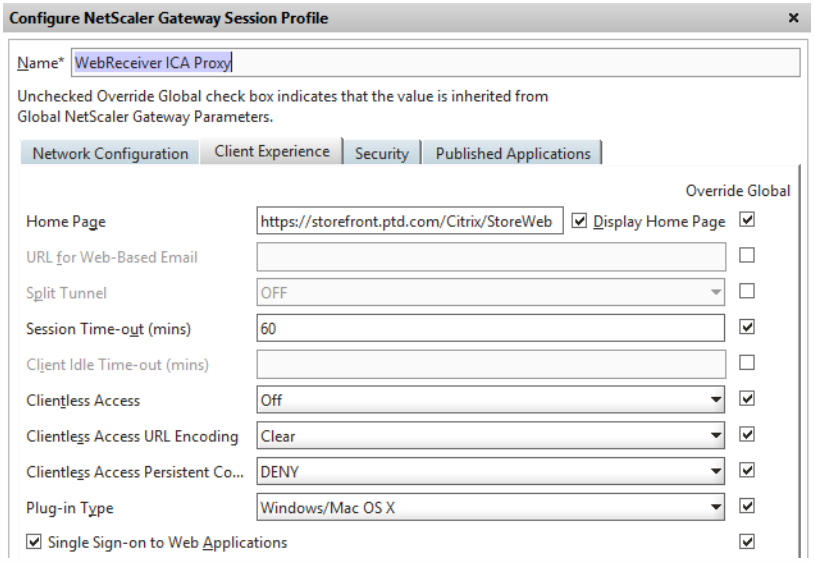
Si usa el proxy de ICA, habilite el modo básico en la página de propiedades del servidor virtual de NetScaler Gateway. Solo se necesita una licencia de plataforma de NetScaler.

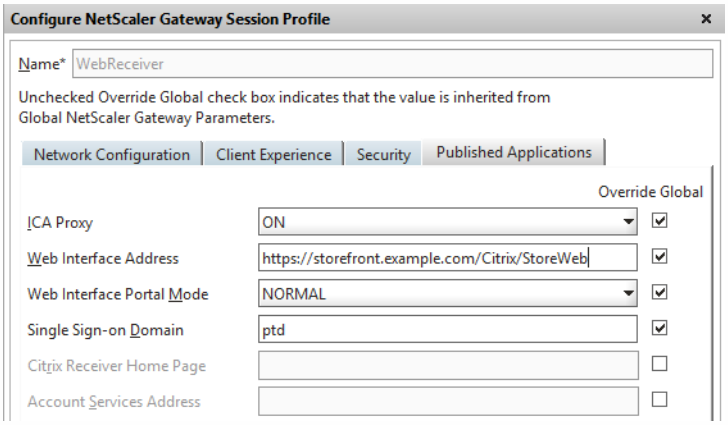
Perfil de Receiver





Perfil de Receiver para Web





Configuración de la URL base del host, la puerta de enlace y el certificado SSL de un servidor StoreFront

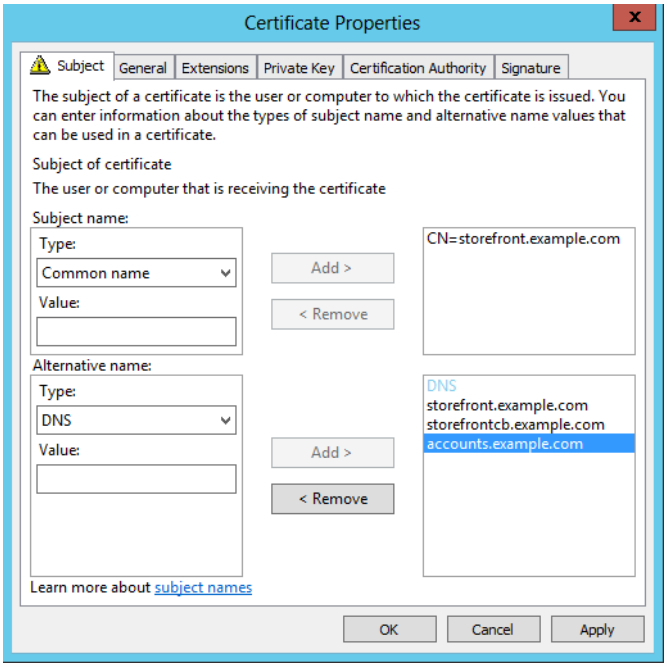
El mismo nombre de dominio completo compartido que se resuelve en el servidor virtual de NetScaler Gateway también debe resolverse directamente en el equilibrador de carga de StoreFront si se ha creado un clúster de StoreFront o si hay una única dirección IP de StoreFront que aloje la tienda.

DNS interno: Cree tres registros A de DNS.

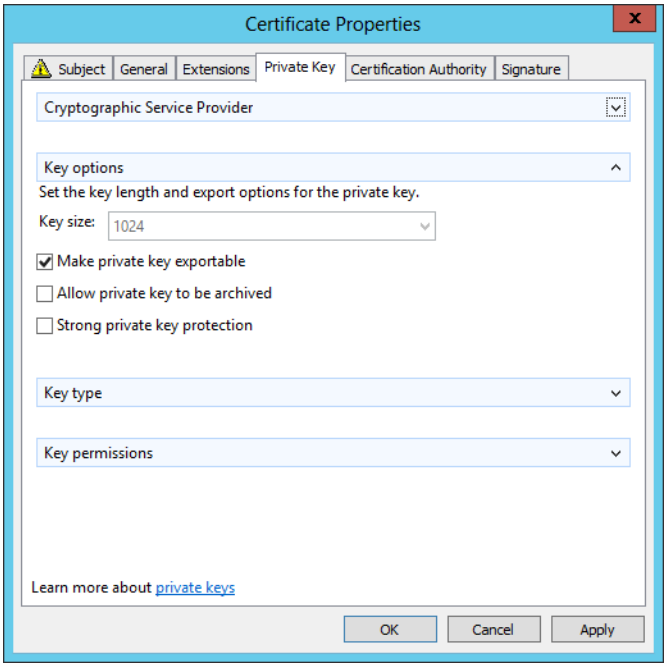
- storefront.example.com debe resolverse en el equilibrador de carga de StoreFront o en la dirección IP única del servidor StoreFront.
- storefrontcb.example.com debe resolverse en la dirección IP virtual del servidor virtual de NetScaler Gateway, de modo que, si existe un firewall entre la DMZ y la red local de la empresa, permita esto.
- accounts.example.com: Cree un alias de DNS para storefront.example.com. También se resuelve en la dirección IP del equilibrador de carga para el clúster de StoreFront o en la dirección IP única del servidor StoreFront.

Certificado de ejemplo de un servidor StoreFront: storefront.example.com

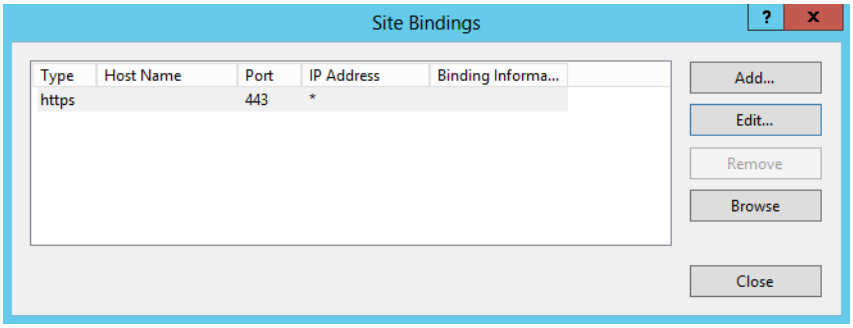
1. Cree un certificado adecuado para el servidor o grupo de servidores StoreFront antes de instalar StoreFront.
2. Agregue el nombre de dominio completo compartido a los campos Nombre común y DNS. Compruebe que coincide con el nombre de dominio completo utilizado en el certificado SSL enlazado al servidor virtual de NetScaler Gateway que ha creado anteriormente o, si no, utilice el mismo certificado enlazado al servidor virtual de NetScaler Gateway.
3. Agregue el alias de la cuenta (accounts.example.com) al certificado como otro nombre SAN. Tenga en cuenta que el alias de la cuenta utilizado en el nombre alternativo de firmante (SAN) es el que se utiliza en el perfil de sesión de NetScaler Gateway del procedimiento anterior (**Perfil y directiva de sesiones de NetScaler Gateway con Receivers nativos**).



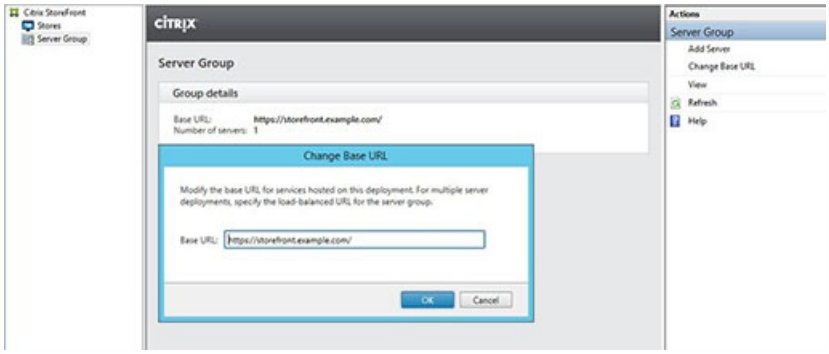
4. Compruebe que la clave privada se puede exportar para que el certificado se pueda transferir a otro servidor StoreFront o a varios nodos de un grupo de servidores StoreFront.



5. Firme el certificado mediante una entidad de certificación (CA) externa como Verisign, o mediante una CA empresarial de la organización, o mediante una CA intermedia.
6. Exporte el certificado en formato PFX e incluya la clave privada.
7. Importe el certificado y la clave privada en el servidor StoreFront. Si va a implementar un clúster de StoreFront de Windows sin equilibrio de carga, importe el certificado en todos los nodos. Si utiliza un equilibrador de carga alternativo, como un servidor virtual de NetScaler con equilibrio de carga, importe el certificado ahí en su lugar.
8. Cree un enlace HTTPS de IIS en el servidor StoreFront y enlácele el certificado SSL importado.



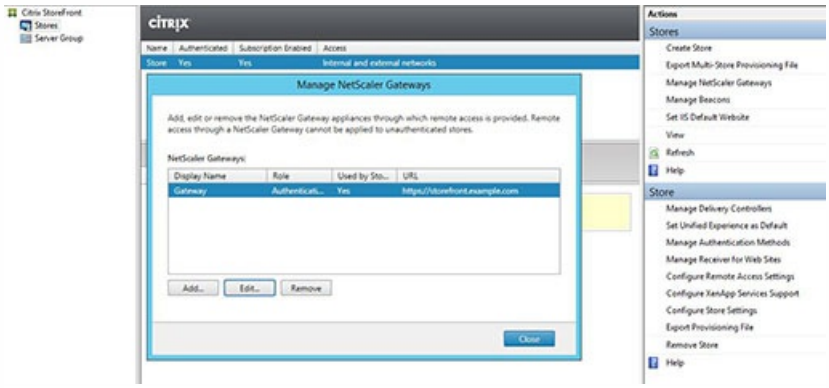
9. Configure la URL base del host en el servidor StoreFront para que coincida con el nombre de dominio completo compartido que ya ha elegido.
   Nota: StoreFront siempre selecciona automáticamente el último nombre alternativo de firmante (SAN) en la lista de nombres alternativos de firmante del certificado. Esto es una sugerencia de URL base del host para ayudar a los administradores de StoreFront y normalmente es correcta. Puede configurarla manualmente con cualquier dirección HTTPS://<FQDN> válida, siempre que exista en el certificado como un nombre SAN. Ejemplo: https://storefront.example.com



Configure NetScaler Gateway en el servidor StoreFront: storefront.example.com

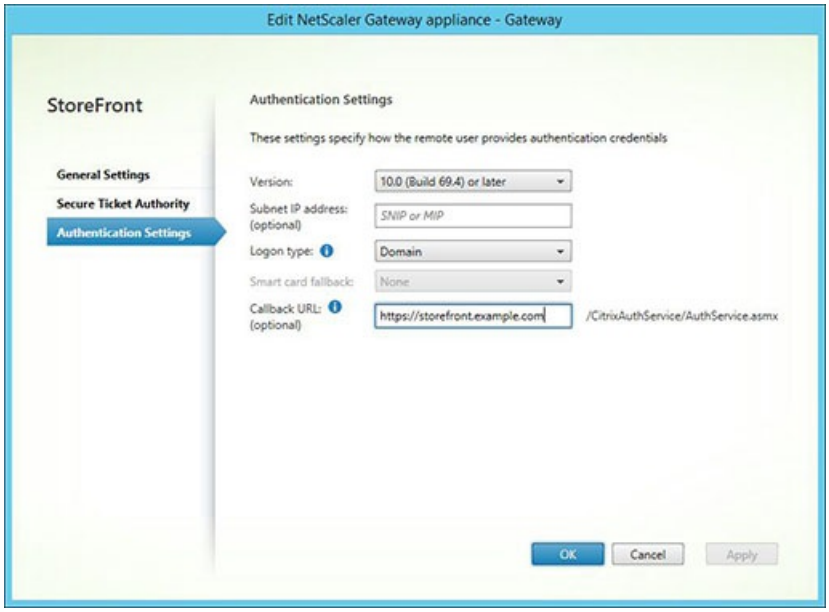
1. En el nodo **Tiendas** , haga clic en **Administrar NetScaler Gateway** en el panel **Acciones**.

2. Seleccione la **puerta de enlace** en la lista y haga clic en **Modificar**.



3. En la página **Parámetros generales**, introduzca el nombre FQDN compartido en el campo **URL de NetScaler Gateway**.

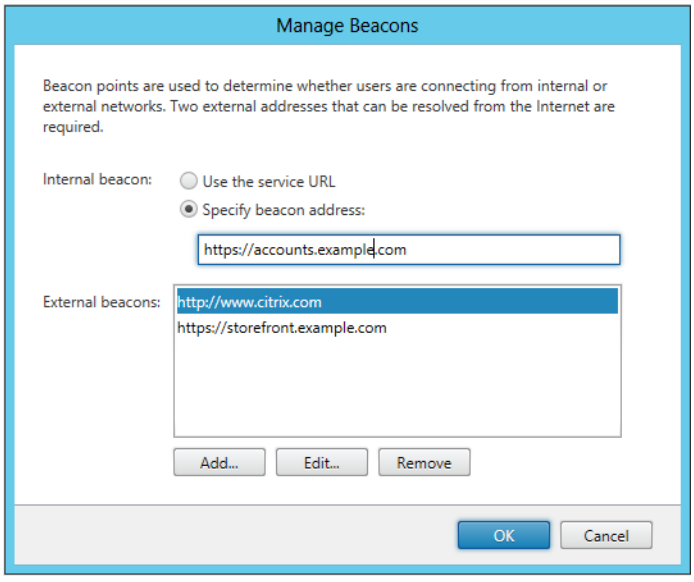
4. Seleccione la ficha **Parámetros de autenticación** e introduzca el nombre FQDN de respuesta en el campo **URL de respuesta**.



5. Seleccione la ficha **Secure Ticket Authority** y asegúrese de que los servidores Secure Ticket Authority (STA) coinciden con la lista de Delivery Controllers ya configurados en el nodo **Tienda**.

6. Habilite el acceso remoto a la tienda.

7. Establezca manualmente la baliza interna para el alias de la cuenta (accounts.example.com) y configúrela de modo que no se pueda resolver desde fuera de la puerta de enlace. El nombre de dominio completo debe ser distinto de la baliza externa que comparten la URL base del host de StoreFront y el servidor virtual de NetScaler Gateway (storefront.example.com). NO utilice el nombre de dominio completo compartido, ya que crea una situación en la que la baliza interna y la baliza externa son idénticas.



8. Si quiere respaldar la detección mediante nombres de dominio completo, siga estos pasos. Si la configuración del archivo de aprovisionamiento es suficiente o si solo está utilizando Receiver para Web, puede omitir los pasos siguientes.

Agregue una entrada adicional en C:\inetpub\wwwroot\Citrix\Authentication\web.config. Hay dos entradas en el archivo web.config de autenticación. Solo la primera entrada del archivo requiere agregar una entrada más para el productor de

tokens de autenticación.

9. Realice una búsqueda de la cadena . Busque la siguiente entrada, agregue la línea que aparece en **negrita**, guarde y cierre el archivo web.config.

.....

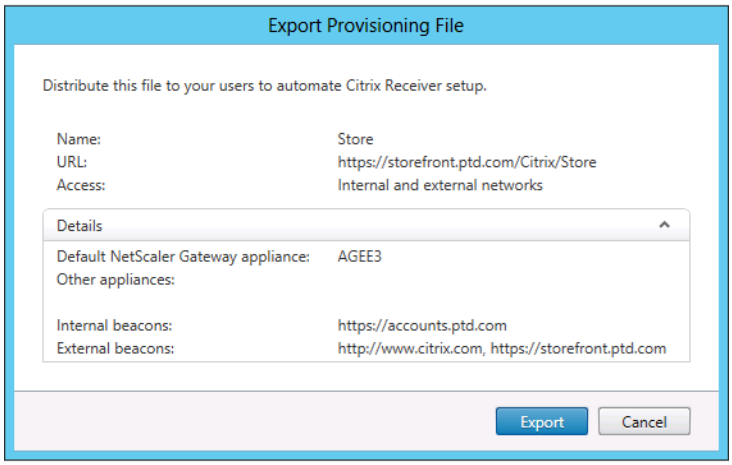
.....

9. En **C:\inetpub\wwwroot\Citrix\Roaming\web.config**.Busque la siguiente entrada, agregue la línea que aparece en **negrita**, guarde y cierre el archivo web.config.

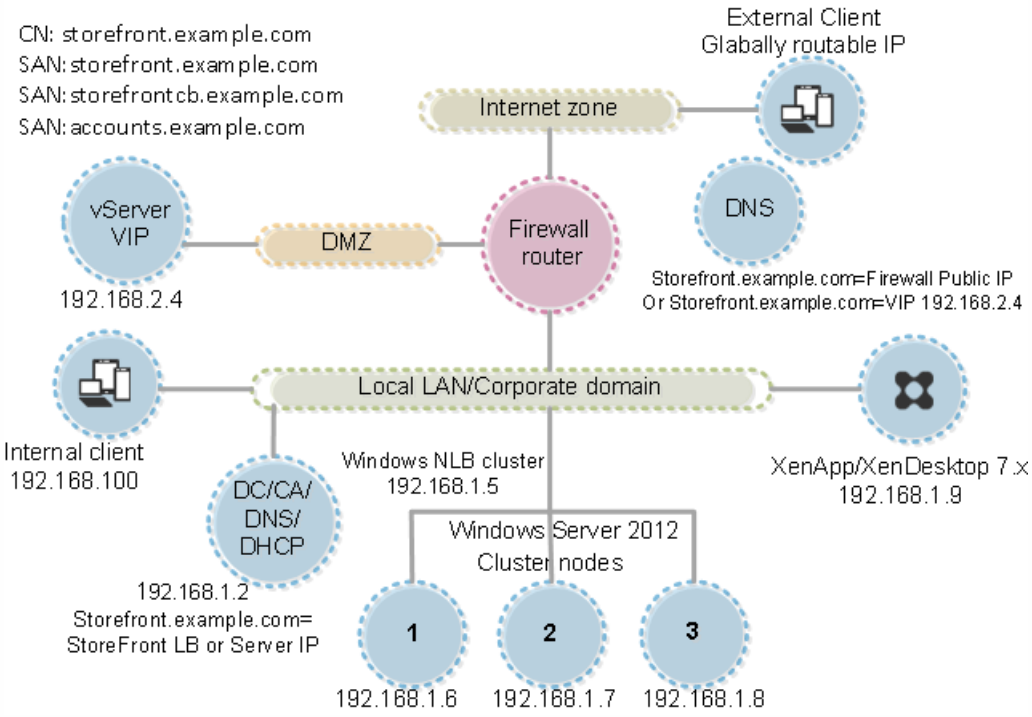
.....

.....

También es posible exportar el archivo .CR de aprovisionamiento del Receiver nativo para la tienda. Así, ya no hay necesidad de la configuración para el primer uso de Receivers nativos. Distribuya este archivo a todos los clientes de Receiver para Windows y Mac.



Si ya hay un Receiver instalado en el cliente, el tipo de archivo .CR se reconoce y, al hacer doble clic en el archivo de aprovisionamiento, este se importa automáticamente.



Configuración del filtro de recursos

Aug 14, 2017

En este tema se explica cómo filtrar recursos de enumeración según el tipo de recurso y las palabras clave. Puede usar este tipo de filtro junto a la personalización más avanzada que ofrece el SDK de personalización de tiendas (Store Customization SDK). Con este SDK puede controlar qué aplicaciones y escritorios se muestran a los usuarios, además de modificar las condiciones de acceso y ajustar los parámetros de inicio. Para más información, consulte el SDK de personalización de tiendas.

Nota: Las consolas de StoreFront y PowerShell no pueden estar abiertas al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.

Configuración del filtro

Configure el filtro con los cmdlets de PowerShell definidos en el módulo StoresModule. Utilice el siguiente snippet de PowerShell para cargar los módulos requeridos:

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

Filtro por tipo

Utilice esto para filtrar la enumeración de recursos por tipo de recurso. Se trata de un filtro inclusivo. Este filtro elimina, del resultado de las enumeraciones de recursos, todos aquellos recursos que no encajen en los tipos especificados. Use los siguientes cmdlets:

Set-DSResourceFilterType. Establece un filtro de enumeración según los tipos de recurso.

Get-DSResourceFilterType. Obtiene una lista de tipos de recursos que StoreFront puede devolver en forma de enumeración.

Nota: Los tipos de recurso se aplican antes de las palabras clave.

Filtro por palabras clave

Utilícelo para filtrar recursos por palabras clave, como los recursos derivados de XenDesktop o XenApp. Las palabras clave se generan desde el marcado en el campo de descripción del recurso correspondiente.

El filtro puede funcionar tanto en modo inclusivo como en modo exclusivo, pero no en ambos. El filtro inclusivo permite la enumeración de recursos que coincidan con las palabras clave configuradas y elimina de la enumeración los recursos que no coincidan. El filtro exclusivo elimina de la enumeración los recursos que coinciden con las palabras clave configuradas. Use los siguientes cmdlets:

Set-DSResourceFilterKeyword: Establece un filtro de enumeración según las palabras clave de los recursos.

Get-DSResourceFilterKeyword: Obtiene la lista de palabras clave del filtro.

Las siguientes palabras clave están reservadas y no se deben usar para el filtrado:

- Automática
- Obligatorio

Para obtener más información sobre las palabras clave, consulte Mejora de la experiencia de usuario y Configuración de la entrega de aplicaciones.

Ejemplos

Este comando utilizará el filtrado para excluir recursos de flujos de trabajo presentes en la enumeración:

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

Este ejemplo aplicará los tipos permitidos de recurso solo a aplicaciones:

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -ExcludeKeywords @("WFS")
```

Configuración mediante archivos de configuración

Aug 14, 2017

Puede usar archivos de configuración para configurar parámetros adicionales de Citrix StoreFront y Citrix Receiver para Web que no se puedan definir en la consola de administración de Citrix StoreFront.

Puede configurar los siguientes parámetros de Citrix StoreFront:

- Habilitación de ICA File Signing
- Inhabilitación de la asociación de tipos de archivo
- Personalización del cuadro de diálogo de inicio de sesión de Citrix Receiver
- Cómo evitar que Receiver para Windows almacene en caché las contraseñas y los nombres de usuario

Puede configurar los siguientes parámetros de Citrix Receiver para Web:

- Cómo se muestran los recursos a los usuarios
- Inhabilitación de la vista de carpetas de Mis aplicaciones

Configuración de StoreFront mediante archivos de configuración

Aug 14, 2017

En este artículo se describen las tareas de configuración adicionales que no se pueden llevar a cabo usando la consola de administración de Citrix StoreFront.

Habilitación de ICA File Signing

Inhabilitación de la asociación de tipos de archivo

Personalización del cuadro de diálogo de inicio de sesión de Citrix Receiver

Cómo evitar que Citrix Receiver para Windows almacene en caché las contraseñas y los nombres de usuario

Habilitación de ICA File Signing

StoreFront proporciona la opción de firmar digitalmente los archivos ICA para que las versiones de Citrix Receiver que admiten esta función puedan verificar que el archivo proviene de una fuente de confianza. Cuando la firma de archivos está habilitada en StoreFront, el archivo ICA que se genera cuando un usuario inicia una aplicación se firma mediante un certificado procedente del almacén de certificados personales del servidor StoreFront. Los archivos ICA pueden firmarse con cualquier algoritmo hash compatible con el sistema operativo que se ejecuta en el servidor StoreFront. Los clientes que no admiten la función o que no están configurados para ICA File Signing ignoran la firma digital. Si el proceso de firma falla, el archivo ICA se genera sin firma digital y se envía a Citrix Receiver, cuya configuración determina si se acepta el archivo sin firmar.

Los certificados deben incluir la clave privada y encontrarse en el período de validez para que puedan utilizarse con ICA File Signing en StoreFront. Si el certificado contiene una extensión de uso de clave, ésta debe permitir que la clave se use para las firmas digitales. Cuando se incluye una extensión de uso mejorado de clave, se debe configurar con firma de código o autenticación del servidor.

Para utilizar la función ICA File Signing, Citrix recomienda el uso de un certificado de firma de código o firma SSL obtenido de una entidad de certificación pública o de la entidad de certificados privada de su organización. Si no puede obtener un certificado adecuado de una entidad de certificación, puede utilizar un certificado SSL existente, como un certificado de servidor, o crear un nuevo certificado de entidad de certificación raíz y distribuirlo a los dispositivos de los usuarios.

De forma predeterminada, la función ICA File Signing está inhabilitada en las tiendas. Para activar la función ICA File Signing, edite el archivo de configuración de la tienda y ejecute comandos de Windows PowerShell. Para obtener más información acerca de la habilitación de ICA File Signing en Citrix Receiver, consulte ICA File Signing: protección contra el inicio de aplicaciones y escritorios desde servidores que no son de confianza.

Nota: Las consolas de StoreFront y PowerShell no pueden estar abiertas al mismo tiempo. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.
Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Asegúrese de que el certificado que desea utilizar para firmar los archivos ICA esté disponible en el almacén de certificados de Citrix Delivery Services del servidor StoreFront y no en el almacén de certificados actual de los usuarios.
2. Utilice un editor de texto para abrir el archivo web.config para la tienda, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storename\, donde storename es el nombre especificado para la tienda durante su creación.
3. Localice la siguiente sección en el archivo.
   ...
4. Incluya información sobre el certificado que debe utilizarse para la firma, como se muestra a continuación.
   certificateid" thumb="certificatethumbprint" /> ...
   Donde certificateid es un valor que le ayudará a identificar el certificado en el archivo de configuración de la tienda y certificatethumbprint es el resultado (o huella digital) de los datos del certificado generado por el algoritmo hash.
5. Localice el siguiente elemento en el archivo.
6. Cambie el valor del atributo enabled a True si quiere habilitar la función ICA File Signing para la tienda. Establezca el valor del atributo certificateId con el ID utilizado para identificar el certificado, es decir certificateid, en el paso 4.
7. Si quiere utilizar un algoritmo hash que no sea SHA-1, establezca el valor del atributo hashAgorithm con sha256, sha384 o sha512, según corresponda.
8. Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell y, en el símbolo del sistema, escriba los siguientes comandos para permitir el acceso del almacén a la clave privada.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands $certificate = Get-DSCertificate "certificatethumbprint" Add-DSCertificateKeyReadAccess -certificate $certificates[0] -accountName "IIS
   Donde certificatethumbprint es el resultado de los datos del certificado generado por el algoritmo hash.

Inhabilitación de la asociación de tipos de archivo

De forma predeterminada, la asociación de tipos de archivo está habilitada en las tiendas para que el contenido se redirija directamente a las aplicaciones suscritas de los usuarios cuando abren archivos locales de los correspondientes tipos. Para inhabilitar la asociación de tipos de archivo, edite el archivo de configuración de la tienda.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Utilice un editor de texto para abrir el archivo web.config para la tienda, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storename\, donde storename es el nombre especificado para la tienda durante su creación.
2. Localice el siguiente elemento en el archivo.
3. Cambie el valor del atributo enableFileTypeAssociation a off para inhabilitar la asociación de tipos de archivo en la tienda.

Personalización del cuadro de diálogo de inicio de sesión de Citrix Receiver

De forma predeterminada, cuando los usuarios de Citrix Receiver inician sesión en una tienda, no se muestra ningún texto de título en el cuadro de diálogo de inicio de sesión. Es posible mostrar el texto predeterminado "Please log on" o redactar un mensaje personalizado propio. Para mostrar y personalizar el texto de título en el cuadro de diálogo de inicio de sesión de Citrix Receiver, edite los archivos para el servicio de autenticación.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Utilice un editor de texto para abrir el archivo UsernamePassword.tfrm para el servicio de autenticación, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\.
2. Localice las siguientes líneas en el archivo.
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
3. Elimine el comentario del enunciado. Para ello, quite las @* en el inicio y las *@ en el final del enunciado tal y como se muestra a continuación.
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   Los usuarios de Citrix Receiver ven el texto de título predeterminado "Please log on", o la versión localizada de este texto, cuando inician sesión en las tiendas donde se utiliza este servicio de autenticación.

4. Para modificar el texto de título, utilice un editor de texto para abrir el archivo ExplicitAuth.resx para el servicio de autenticación que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\.
5. Localice los siguientes elementos en el archivo. Edite el texto dentro del elemento para modificar el texto de título que los usuarios ven en el cuadro de diálogo de inicio de sesión de Citrix Receiver al acceder a tiendas en las que se utiliza este servicio de autenticación.
   My Company Name
   Para modificar el texto de título del cuadro de diálogo de inicio de sesión de Citrix Receiver para los usuarios con otras configuraciones regionales, edite los archivos ExplicitAuth traducidos.languagecode.resx, donde languagecode es el identificador de idioma.

Cómo evitar que Citrix Receiver para Windows almacene en caché las contraseñas y los nombres de usuario

De manera predeterminada, Citrix Receiver para Windows almacena las contraseñas de los usuarios cuando inician sesión en las tiendas de StoreFront. Para evitar que Citrix Receiver para Windows, pero no Citrix Receiver para Windows Enterprise, almacene en caché las contraseñas de los usuarios, edite los archivos del servicio de autenticación.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Use un editor de textos para abrir el archivo inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrm.
2. Localice la siguiente línea en el archivo.
   @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey: "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked: ControlValue("SaveCredentials"))
3. Agregue marcas de comentario en la declaración, como se muestra a continuación.
   Los usuarios de Citrix Receiver para Windows deben introducir sus contraseñas cada vez que inician sesión en tiendas que utilizan este servicio de autenticación. Esta configuración no se aplica a Citrix Receiver para Windows Enterprise.

> **Advertencia**
>
> El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

De manera predeterminada, Citrix Receiver para Windows rellena el formulario automáticamente con el último nombre de usuario que se utilizó. Para evitar que el campo de nombre de usuario se rellene de este modo, edite el Registro en el dispositivo del usuario:

1. Cree un valor REG_SZ HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Defina su valor como "false".

Configuración de los sitios de Citrix Receiver para Web mediante los archivos de configuración

Aug 14, 2017

En este artículo, se describen las tareas de configuración adicionales para los sitios de Citrix Receiver para Web que no se pueden llevar a cabo con la consola de administración de Citrix StoreFront.

Configuración de la forma en que se muestran los recursos para los usuarios

Cuando tanto escritorios como aplicaciones están disponibles desde un sitio de Citrix Receiver para Web, aparecen vistas separadas de los escritorios y las aplicaciones de forma predeterminada. Los usuarios ven la vista de escritorio primero al iniciar sesión en el sitio. Si solo hay un escritorio disponible para un usuario, independientemente de si hay aplicaciones también disponibles en un sitio, dicho escritorio se inicia automáticamente cuando el usuario inicia sesión. Para cambiar estos parámetros, edite el archivo de configuración del sitio.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Utilice un editor de texto para abrir el archivo web.config del sitio de Citrix Receiver para Web, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storenameWeb\, donde storename es el nombre especificado para la tienda en el momento de su creación.
2. Localice el siguiente elemento en el archivo.

3. Cambie el valor de los atributos showDesktopsView y showAppsView a false para evitar que los escritorios y las aplicaciones, respectivamente, se muestren a los usuarios, aunque sea posible acceder a estos recursos desde el sitio. Si las vistas de escritorios y aplicaciones están habilitadas, establezca el valor del atributo defaultView en apps para que se muestre primero la vista de aplicaciones cuando los usuarios inicien sesión en el sitio.
4. Localice el siguiente elemento en el archivo.

5. Cambie el valor del atributo autoLaunchDesktop a false para evitar que los sitios de Receiver para Web inicien automáticamente un escritorio cuando un usuario inicie sesión en el sitio y solo haya un escritorio disponible para ese usuario.
   Cuando el atributo autoLaunchDesktop está establecido en true e inicia sesión un usuario para el que solo hay un escritorio disponible, las aplicaciones de dicho usuario no se vuelven a conectar, independientemente de la configuración del control del espacio de trabajo.

Nota: Para permitir que en los sitios de Citrix Receiver para Web los escritorios se inicien automáticamente, los usuarios que acceden al sitio mediante Internet Explorer deben agregar el sitio a las zonas de Intranet local o Sitios de confianza.

Inhabilitación de la vista de carpetas de Mis aplicaciones

De forma predeterminada, Citrix Receiver para Web muestra la vista de carpetas de Mis aplicaciones para tiendas no autenticadas (acceso para usuarios no autenticados) y obligatorias (todas las aplicaciones publicadas están disponibles en la pantalla principal sin que los usuarios estén suscritos a ellas). Esta vista muestra las aplicaciones en una jerarquía de carpetas e incluye una ruta de acceso al árbol de navegación.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración

del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. Utilice un editor de texto para abrir el archivo web.config del sitio de Citrix Receiver para Web, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storenameWeb\, donde storename es el nombre especificado para la tienda en el momento de su creación.
2. Localice el siguiente elemento en el archivo.
3. Cambie el valor del atributo enableAppsFolderView a false para inhabilitar la vista de la carpeta Mis aplicaciones en Citrix Receiver para Web.

Protección de la implementación de StoreFront

Aug 14, 2017

En este artículo se muestran las áreas que pueden afectar la seguridad del sistema durante la implementación y la configuración de StoreFront.

Configuración de Microsoft Internet Information Services (IIS)

StoreFront puede configurarse con una configuración restringida de IIS. Esta no es la configuración predeterminada de IIS.

Extensiones de archivo:
Puede prohibir extensiones de nombre de archivo no incluidas en la lista.

StoreFront requiere estas extensiones de nombre de archivo en la opción Filtro de solicitudes:

- . (extensión en blanco)
- .appcache
- .aspx
- .cr
- .css
- .dtd
- .gif
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- archivo
- .xml

Si la descarga o la actualización de Citrix Receiver está habilitada para Citrix Receiver para Web, StoreFront también requiere estas extensiones de nombre de archivo:

- .dmg
- .exe

Si Citrix Receiver para HTML5 está habilitado, StoreFront también requiere estas extensiones de nombre de archivo:

- .eot
- .ttf
- .woff

StoreFront requiere los siguientes verbos de HTTP en Filtro de solicitudes. Puede prohibir los verbos que no se encuentren en la lista.

- GET
- POST
- HEAD

StoreFront no requiere:

- Filtros de ISAPI
- Extensiones ISAPI
- Programas CGI
- Programas FastCGI

> **Important**
>
> - StoreFront requiere Plena confianza. No configure el nivel de confianza de .NET con un nivel Alto o inferior.
> - StoreFront no da respaldo al uso de grupos de aplicaciones separados para cada sitio. No modifique estos parámetros de sitio.

Configuración de derechos de usuario

Cuando se instala StoreFront, sus grupos de aplicaciones reciben el derecho de **Iniciar sesión como un servicio**, y los privilegios siguientes: **Ajustar las cuotas de la memoria para un proceso, Generar auditorías de seguridad** y **Reemplazar un símbolo (token) de nivel de proceso**. Este es el comportamiento normal de instalación cuando se crean los grupos de aplicaciones.

No es necesario que cambie estos derechos de usuario. Estos privilegios no se usan en StoreFront y están inhabilitados automáticamente.

La instalación de StoreFront crea los siguientes servicios de Windows:

- 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)

Si configura la delegación restringida de Kerberos en StoreFront para XenApp 6.5, esto crea el servicio Citrix StoreFront Protocol Transition (NT SERVICE\SYSTEM). Este servicio requiere un privilegio que normalmente no se concede a servicios Windows.

Configuración de parámetros de servicios

Los servicios Windows de StoreFront enumerados arriba en la sección "Configuración de derechos de usuario" están configurados para iniciar sesión con la identidad NETWORK SERVICE (Servicio de red). El servicio Citrix StoreFront Protocol Transition inicia sesión como SYSTEM (Sistema). No cambie esta configuración.

Configuración de la pertenencia a grupos

La instalación de StoreFront agrega los siguientes servicios al grupo de seguridad de Administradores:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)

La pertenencia de estos grupos es necesaria para que StoreFront funcione correctamente, para:

- Crear, exportar, importar y eliminar certificados y definir permisos de acceso en ellos
- Leer y escribir en el Registro de Windows
- Agregar y quitar ensamblados de Microsoft .NET Framework en la caché Global Assembly Cache (GAC)
- Acceder a la carpeta **Archivos de programa\Citrix***<Ubicación de StoreFront>*
- Agregar, modificar y quitar identidades de grupos de aplicaciones de IIS y aplicaciones Web de IIS
- Agregar, modificar y quitar grupos de seguridad local y reglas de firewall
- Agregar y quitar servicios de Windows y complementos de PowerShell
- Registrar puntos finales de Microsoft Windows Communication Framework (WCF)

En actualizaciones de StoreFront, esta lista de operaciones puede cambiarse sin previo aviso.

La instalación de StoreFront también crea los siguientes grupos de seguridad locales:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSUsers
- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront mantiene la pertenencia de los miembros de estos grupos de seguridad. Se utilizan para el control de acceso dentro de StoreFront y no se aplican a recursos de Windows tales como archivos y carpetas. No modifique los miembros de estos grupos.

Certificados en StoreFront

Certificados de servidor

Los certificados de servidor se usan para identificar las máquinas y para aplicar seguridad TLS (Transport Layer Security) al transporte de datos en StoreFront. Si decide habilitar ICA File Signing, StoreFront también puede utilizar los certificados para firmar los archivos ICA de forma digital.

Para habilitar la detección de cuentas basada en direcciones de correo electrónico en caso de usuarios que instalan por primera vez Citrix Receiver en un dispositivo, debe instalar un certificado de servidor válido en el servidor StoreFront. También es necesario que la cadena completa al certificado raíz sea válida. Para una experiencia de usuario óptima, instale un certificado con una entrada de Sujeto o Nombre alternativo del sujeto con el valor **discoverReceiver.domain**, donde domain es el dominio de Microsoft Active Directory que contiene las cuentas de correo electrónico de los usuarios. Aunque se puede usar un certificado comodín para el dominio que contiene las cuentas de correo electrónico de los usuarios, primero es necesario asegurarse de que la implementación de dichos certificados está permitida por las directivas de seguridad de la empresa. También se pueden usar otros certificados para el dominio de las cuentas de correo electrónico de los usuarios, pero los usuarios verán un cuadro de diálogo de advertencia acerca de los certificados cuando Citrix Receiver se

conecte por primera vez al servidor StoreFront. La detección de cuentas basada en direcciones de correo electrónico no se puede utilizar con ninguna otra identidad de certificado. Para obtener más información, consulte Configuración de la detección de cuentas basada en direcciones de correo electrónico.

Si los usuarios configuran sus cuentas introduciendo las direcciones URL de la tienda directamente en Citrix Receiver y no usan la detección de cuentas basada en direcciones de correo electrónico, el certificado del servidor StoreFront tiene que ser válido solamente para ese servidor y debe tener una cadena válida hasta el certificado raíz.

Certificados de administración de tokens

Tanto los servicios de autenticación como las tiendas requieren certificados para la administración de tokens. StoreFront genera un certificado autofirmado cuando se crean servicios de autenticación o tiendas. Los certificados autofirmados que genera StoreFront no deben utilizarse para otros fines.

Certificados de Citrix Delivery Services

StoreFront guarda una serie de certificados en un almacén de certificados de Windows personalizado (Citrix Delivery Services). Los siguientes servicios usan estos certificados: Citrix Configuration Replication Service, Citrix Credential Wallet Service, y Citrix Subscriptions Store Service. Cada servidor StoreFront de un clúster tiene una copia de estos certificados. Estos servicios no dependen de TLS para las comunicaciones seguras y no se usan como certificados TLS. Estos certificados se crean cuando se crea una tienda de StoreFront o cuando se instala StoreFront. No modifique el contenido de este almacén de certificados de Windows.

Certificados de firma de código

StoreFront incluye una serie de scripts de PowerShell (.ps1) en la carpeta \Scripts. La instalación predeterminada de StoreFront no hace uso de estos scripts. Con ellos se pueden simplificar los pasos de configuración para tareas específicas que se llevan a cabo con poca frecuencia. Estos scripts están firmados, lo que permite que StoreFront respalde la directiva de ejecución de PowerShell. Recomendamos usar la directiva **AllSigned**. (La directiva **Restricted** no recibe respaldo, porque impide la ejecución de los scripts de PowerShell). StoreFront no modifica la directiva de ejecución de PowerShell.

Aunque StoreFront no instala un certificado de firma de código en el almacén Editores de confianza, Windows puede agregar automáticamente el certificado de firma de código ahí. Esto ocurre cuando el script de PowerShell se ejecuta con la opción **Ejecutar siempre**. (Si selecciona la opción **No ejecutar nunca**, el certificado se agrega al almacén de Certificados en los que no se confía, y los scripts de PowerShell de StoreFront no se ejecutarán). Una vez que el certificado de firma de código ha sido agregado al almacén Editores de confianza, Windows ya no comprueba su caducidad. Puede quitar este certificado del almacén Editores de confianza después de que las tareas de StoreFront se hayan completado.

Comunicaciones de StoreFront

En un entorno de producción, Citrix recomienda el uso del protocolo de seguridad de Internet (IPsec) o protocolos HTTPS para proteger la transferencia de los datos entre StoreFront y los servidores. IPsec es un conjunto de extensiones estándar para el protocolo de Internet. Proporciona comunicaciones autenticadas y cifradas con integridad de datos y protección contra reproducción. Como IPsec es un conjunto de protocolos de capa de red, los protocolos con niveles más elevados pueden utilizarlo sin realizar ninguna modificación. HTTPS utiliza protocolos SSL y TLS para proporcionar un cifrado de datos avanzado.

El Traspaso SSL se puede usar para proteger el tráfico de datos entre StoreFront y los servidores de XenApp. El Traspaso SSL es un componente predeterminado de XenApp que lleva a cabo la autenticación del host y el cifrado de datos.

Citrix recomienda proteger la comunicación entre los dispositivos de los usuarios y StoreFront mediante NetScaler Gateway

y HTTPS. Para utilizar HTTPS, StoreFront requiere que la sesión de Microsoft Internet Information Services (IIS) que aloja el servicio de autenticación y las tiendas asociadas esté configurada para HTTPS. Sin una configuración de IIS adecuada, StoreFront utiliza HTTP para las comunicaciones. Citrix recomienda encarecidamente no habilitar conexiones de usuario no seguras a StoreFront en un entorno de producción.

Separación de seguridad de StoreFront

Si implementa aplicaciones Web en el mismo dominio Web (nombre de dominio y puerto) que StoreFront, cualquier posible problema de seguridad de esas aplicaciones Web podrían afectar a su vez a la seguridad de la implementación de StoreFront. Cuando se necesita un mayor nivel de seguridad es necesario separarlos: Citrix recomienda implementar StoreFront en un dominio Web aparte.

ICA File Signing

StoreFront ofrece la opción de firmar de forma digital los archivos ICA mediante un certificado especificado en el servidor, para que las versiones de Citrix Receiver que admiten esta función puedan verificar que el archivo proviene de una fuente de confianza. Los archivos ICA se pueden firmar con cualquier algoritmo hash que admita el sistema operativo que se ejecuta en el servidor StoreFront, incluidos SHA-1 y SHA-256. Para obtener más información, consulte Habilitación de la firma de archivos ICA.

Cambio de contraseña del usuario

Puede permitir el cambio de contraseñas por parte de los usuarios de los sitios de Receiver para Web que inicien sesión con credenciales de dominio de Active Directory. Una vez concedido el permiso, los usuarios podrán cambiarlas en cualquier momento o solo cuando hayan caducado. No obstante, esto deja funciones de seguridad importantes al alcance de cualquier persona que pueda acceder a las tiendas que utilizan el servicio de autenticación. Si su organización cuenta con una directiva de seguridad que solo permite utilizar las funciones de cambio de contraseñas de los usuarios para uso interno, asegúrese de que no se pueda acceder a las tiendas desde fuera de la red corporativa. Al crear el servicio de autenticación, la configuración predeterminada impide que los usuarios de los sitios de Receiver para Web cambien sus contraseñas, incluso aunque hayan caducado. Para obtener más información, consulte Mejora de la experiencia de usuario.

Personalizaciones

Para reforzar la seguridad, no escriba personalizaciones que carguen contenido o scripts desde servidores que no estén bajo su control. Copie el contenido o el script en la carpeta de personalización del sitio de Citrix Receiver para Web que está personalizando. Si StoreFront está configurado para conexiones HTTPS, asegúrese de que todos los enlaces con el contenido o scripts personalizados usan también HTTPS.

Exportación e importación de la configuración de StoreFront

Aug 14, 2017

Puede exportar la configuración completa de una implementación de StoreFront. Esto incluye tanto implementaciones de un único servidor como implementaciones con un grupo de servidores. Si una implementación existente ya está presente en el servidor que realiza la importación, la configuración actual se borra y se sustituye por la configuración contenida en el archivo de copia de seguridad. Si el servidor de destino es una instalación limpia con los valores predeterminados de fábrica, se crea una nueva implementación usando la configuración importada almacenada en la copia de seguridad. La copia de seguridad de la configuración exportada es un archivo .zip único si no está cifrada, o un archivo .ctxzip si se eligió cifrar el archivo de copia de seguridad al crearlo.

Asuntos a considerar al importar y exportar una configuración de StoreFront

Objetos de credenciales de PowerShell utilizados para el cifrado y descifrado de copias de seguridad de StoreFront

Cmdlets de PowerShell

Ejemplos de exportación e importación de configuraciones

Asuntos a considerar al importar y exportar una configuración de StoreFront

- ¿Quiere usar la URL base de host contenida en el archivo de copia de seguridad, o quiere especificar una URL base de host nueva para usarla en el servidor donde se importa la configuración?
- ¿Está usando actualmente algún ejemplo de SDK de autenticación publicado de Citrix, por ejemplo, personalizaciones para autenticación con palabra mágica o para autenticación con productos de terceros? En ese caso, debe instalar esos paquetes en TODOS los servidores donde se importa la configuración ANTES de importar la configuración que contenga métodos de autenticación adicionales. La importación de la configuración falla si los paquetes del SDK de autenticación no están instalados en los servidores donde se importa la misma. Si importa una configuración en un grupo de servidores, instale los paquetes de autenticación en todos los miembros del grupo.
- Puede cifrar y descifrar los archivos de copia de seguridad. Los cmdlets PowerShell de importación y exportación dan respaldo a ambos casos de uso.
- Puede descifrar copias de seguridad cifradas (.ctxzip) más adelante, pero StoreFront no puede volver a cifrar archivos de copia de seguridad no cifrados (.zip). Si se requiere una copia de seguridad cifrada, realice la exportación de nuevo usando un objeto de credenciales que contenga la contraseña que usted quiera.
- El ID de sitio del sitio Web de IIS donde StoreFront está instalado actualmente (servidor de exportación) debe coincidir con el ID de sitio del sitio Web de IIS de destino (servidor de importación) donde se quiere restaurar la copia de seguridad de la configuración de StoreFront.

Objetos de credenciales de PowerShell utilizados para el cifrado y descifrado de copias de seguridad de StoreFront

Un objeto de credenciales de PowerShell se compone de un nombre de usuario y una contraseña de una cuenta de Windows. Los objetos de credenciales de PowerShell garantizan que su contraseña queda protegida en memoria.

> **Nota**

> Para cifrar un archivo de copia de seguridad de configuración, necesita solo la contraseña para realizar el cifrado y el descifrado. El nombre de usuario guardado con el objeto de credenciales no se usa. Debe crear un objeto de credenciales que contenga la misma contraseña dentro de las sesiones de PowerShell que se utiliza **en los servidores de exportación y de importación**. Dentro del objeto de credenciales puede especificar cualquier usuario.

PowerShell requiere la especificación de un usuario al crear un nuevo objeto de credenciales. Este ejemplo de código obtiene simplemente el usuario de Windows de la sesión actual.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$Password = $Password | ConvertTo-SecureString -asPlainText -Force
$CredObject = New-Object System.Management.Automation.PSCredential($User,$Password)
```

Cmdlets de PowerShell

Export-STFConfiguration

Parámetro	Descripción
-TargetFolder	La ruta de exportación al archivo de copia de seguridad. Ejemplo: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Especifica un objeto de credenciales para crear un archivo de copia de seguridad .ctxzip durante la exportación. El objeto de credenciales de PowerShell debe contener la contraseña que se usará para el cifrado y el descifrado. No use **-Credential** al mismo tiempo que el parámetro **-NoEncryption**. Ejemplo: $CredObject
-NoEncryption (conmutador)	Especifica que el archivo de copia de seguridad debe ser un archivo .zip no cifrado. No use **-NoEncryption** al mismo tiempo que el parámetro **-Credential**.
-ZipFileName	El nombre del archivo de copia de seguridad de la configuración de StoreFront. No agregue ninguna extensión de archivo como .zip o .ctxzip. La extensión del archivo se agrega automáticamente dependiendo de si se especificó el parámetro **-Credential** o el parámetro **-NoEncryption** durante la exportación. Por ejemplo: "copiaSeguridad"
-Force (booleano)	Este parámetro sobrescribe automáticamente los archivos de copia de seguridad con el mismo nombre de archivo que los ya existentes en la ubicación de exportación especificada.

Important

El parámetro **-SiteID** de StoreFront 3.5 pasó a ser obsoleto en la versión 3.6. Ya no es necesario especificar el **ID de sitio (SiteID)** cuando se realiza una importación, porque siempre se usará el parámetro SiteID contenido en el archivo de copia de seguridad. Asegúrese de que el ID de sitio coincide con el sitio Web de StoreFront existente ya configurado dentro de IIS en el servidor de importación. La importación de configuraciones desde **SiteID 1** a **SiteID 2** (o viceversa) NO reciben respaldo.

Import-STFConfiguration

Parámetro	Descripción
-ConfigurationZip	La ruta completa del archivo de copia de seguridad que quiere importar. Esto debe incluir la extensión del archivo. Use .zip para copias de seguridad no cifradas y .ctxzip para las cifradas. Por ejemplo: "$env:userprofile\desktop\backup.ctxzip"
-Credential (PSCredential Object)	Especifique un objeto de credenciales para descifrar una copia de seguridad cifrada durante la importación. Ejemplo: $CredObject
-HostBaseURL	Si se incluye este parámetro, se usará la URL base de host que usted especifique en lugar de usarse la URL base de host del servidor desde donde se realiza la exportación. Por ejemplo: "https://.ejemplo.com"

Unprotect-STFConfigurationBackup

Parámetro	Descripción
-TargetFolder	La ruta de exportación al archivo de copia de seguridad. Ejemplo: "$env:userprofile\desktop\"
-Credential (PSCredential Object)	Use este parámetro para crear una copia no cifrada del archivo de copia de seguridad cifrado. Especifique el objeto de credenciales de PowerShell que contiene la contraseña que debe usarse para el descifrado. Ejemplo: $CredObject

-EncryptedConfigurationZip	La ruta completa del archivo de copia de seguridad cifrado que quiere descifrar. Debe especificar la extensión de archivo .ctxzip. Por ejemplo: "$env:userprofile\desktop\backup.ctxzip"
-OutputFolder	La ruta para crear una copia no cifrada (.zip) del archivo de copia de seguridad cifrado (.ctxzip). El archivo cifrado de copia de seguridad original se conserva para poder volver a utilizarlo. No especifique ningún nombre de archivo ni una extensión de archivo para la copia no cifrada. Ejemplo: "$env:userprofile\desktop\"
-Force (booleano)	Este parámetro sobrescribe automáticamente los archivos de copia de seguridad con el mismo nombre de archivo que los ya existentes en la ubicación de exportación especificada.

Ejemplos de exportación e importación de configuraciones

Importar el SDK de StoreFront en la sesión actual de PowerShell

Abra el entorno ISE (Integrated Scripting Environment) de PowerShell en el servidor StoreFront y ejecute:

```
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$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
```

Escenarios de un solo servidor

Crear una copia de seguridad no cifrada de una configuración existente en el Servidor A y restaurarla sobre la misma implementación.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -zipFileName "backup" -NoEncryption
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.zip"
```

Crear una copia de seguridad cifrada de una configuración existente en el Servidor A y restaurarla sobre la misma implementación.

```
# 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
```

Desproteger un archivo cifrado de copia de seguridad existente

```
$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
```

Hacer una copia de seguridad de una configuración existente en el Servidor A y restaurarla en una nueva implementación con valores predeterminados de fábrica en el Servidor B

El servidor B es una nueva implementación que va a coexistir con el servidor A. Especifique el parámetro **-HostBaseURL**.El servidor B es una instalación limpia de StoreFront con los valores predeterminados de fábrica.

1. Cree un objeto de credenciales de PowerShell y exporte una copia cifrada de la configuración del servidor A.
2. Cree un objeto de credenciales de PowerShell en el servidor B usando la misma contraseña que usó para cifrar la copia de seguridad.
3. Descifre e importe la configuración del servidor A en el servidor B usando el parámetro **-HostBaseURL**.

    ```
    Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
    HostBaseURL "https://serverB.example.com
    ```

Hacer una copia de seguridad de una configuración existente en el Servidor A y usarla para sobrescribir una implementación existente en el Servidor B

El servidor B es una implementación ya existente que tiene una configuración obsoleta. Use la configuración del servidor A para actualizar el servidor B. El servidor B va a coexistir con el servidor A. Especifique el parámetro **-HostBaseURL** .

1. Cree un objeto de credenciales de PowerShell y exporte una copia cifrada de la configuración del servidor A.
2. Cree un objeto de credenciales de PowerShell en el servidor B usando la misma contraseña que usó para cifrar la copia de seguridad.
3. Descifre e importe la configuración del servidor A en el servidor B usando el parámetro **-HostBaseURL**.

    ```
    Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" –Credential $CredObject -
    HostBaseURL "https://servidorB.ejemplo.com"
    ```

Crear un clon de una implementación existente con la misma URL base de host, como cuando se quiere actualizar a un nuevo SO de servidor y retirar una implementación de StoreFront obsoleta

El servidor 2012R B es una nueva implementación con la que se quiere reemplazar al servidor 2008R2 A, que está obsoleto. Use el parámetro HostBaseURL del archivo de copia de seguridad. No use el parámetro **-HostBaseURL** durante la importación.El servidor B es una instalación limpia de StoreFront con los valores predeterminados de fábrica.

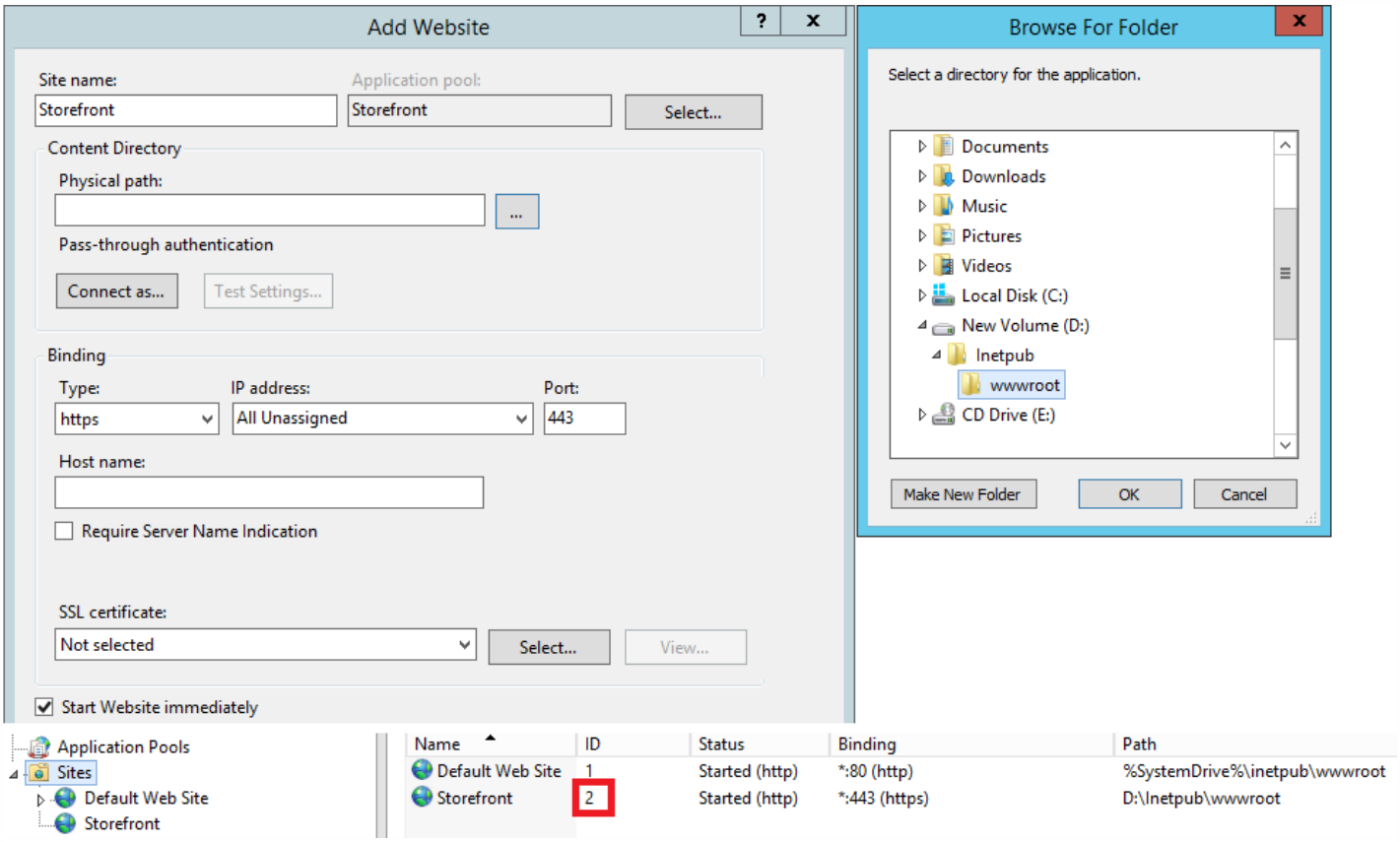
1. Cree un objeto de credenciales de PowerShell y exporte una copia cifrada de la configuración del servidor 2008R2 A.
2. Cree un objeto de credenciales de PowerShell en el servidor 2012R2 B usando la misma contraseña que usó para cifrar la copia de seguridad.
3. Descifre e importe la configuración del servidor 2008R2 A en el servidor 2012R2 B sin usar el parámetro **-HostBaseURL**.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
```

StoreFront ya está implementado en un sitio Web IIS personalizado. Restaurar la configuración en otra implementación de sitio Web personalizado.

El servidor A tiene StoreFront implementado en una ubicación de sitio Web personalizada, en lugar de ubicarse en el sitio Web predeterminado de IIS. El ID de sitio de IIS para el segundo sitio Web creado en IIS es 2. La ruta física del sitio Web de StoreFront puede estar en otra unidad no perteneciente al sistema, como D:\, o en la unidad predeterminada del sistema C:\, pero debe usar un ID de sitio de IIS mayor que 1.

Se ha configurado un nuevo sitio Web llamado StoreFront dentro de IIS, que usa **SiteID = 2**. StoreFront ya está implementado en el sitio Web personalizado y su ruta física se encuentra en la unidad D:\inetpub\wwwrooot\.



1. Cree un objeto de credenciales de PowerShell y exporte una copia cifrada de la configuración del servidor A.
2. En el servidor B, configure IIS con un nuevo sitio Web llamado **StoreFront**, que también use **SiteID 2**.
3. Cree un objeto de credenciales de PowerShell en el servidor B usando la misma contraseña que usó para cifrar la copia de seguridad.
4. Descifre e importe la configuración del servidor A en el servidor B usando el parámetro **-HostBaseURL**. El ID de sitio que

contiene la copia de seguridad es el ID que se utiliza y debe coincidir con el sitio Web de destino donde se quiere importar la configuración de StoreFront.

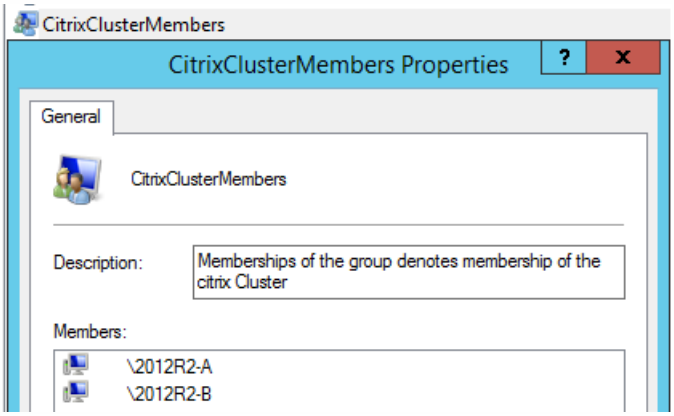
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://serverB.example.com"
```

Escenarios con grupos de servidores

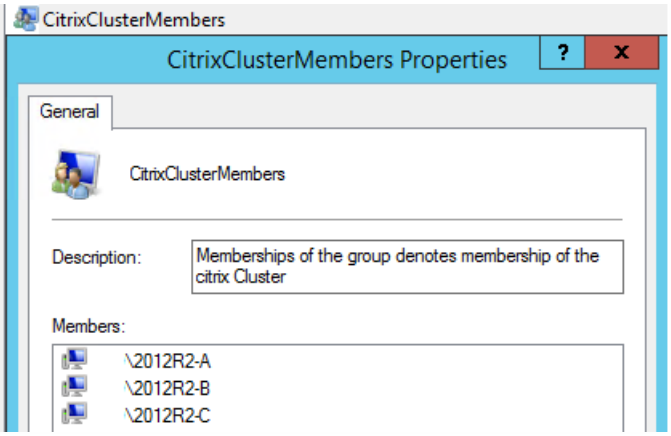
Escenario 1: Hacer una copia de seguridad de la configuración de un grupo de servidores existente y restaurarla más tarde sobre la implementación del mismo grupo de servidores.

Anteriormente se hizo una copia de seguridad de la configuración, cuando el grupo de servidores solo tenía dos servidores StoreFront, 2012R2-A y 2012R2-B. En el archivo de la copia de seguridad se incluye el registro **CitrixClusterMembership** correspondiente al momento en que se hizo la copia, que contiene solo los dos servidores originales 2012R2-A y 2012R2-B. Para incrementar la capacidad del negocio, posteriormente a la creación de esa copia de seguridad original, la implementación del grupo de servidores StoreFront ha aumentado de tamaño y se ha agregado un nodo 2012R2-C al grupo de servidores. La configuración de StoreFront subyacente del grupo de entrega que está guardada en la copia de seguridad no ha cambiado. La información acerca de miembros del grupo CitrixClusterMembership de tres servidores debe conservarse, aunque se importe la antigua copia de seguridad que contiene solo los dos nodos originales del grupo de servidores. Durante la importación, se conserva la información de miembros del clúster CitrixClusterMembership y luego se vuelve a copiar, una vez que la configuración se ha importado correctamente en el servidor principal. La importación también conserva la información de miembros del clúster CitrixClusterMembership aunque se hayan quitado nodos del grupo de servidores posteriormente a la creación de la copia de seguridad original.

1. Exporte la configuración del grupo de servidores 1 desde 2012R2-A, que es el servidor principal utilizado para administrar todo el grupo de servidores.



2. Más tarde, se agrega un servidor adicional, 2012R2-C al grupo de servidores existente.



3. La configuración del grupo de servidores debe restaurarse a un estado de funcionamiento correcto previo conocido. StoreFront hace una copia de seguridad del clúster actual CitrixClusterMembership de tres servidores durante el proceso de importación, y luego la restaura, una vez completada correctamente la importación.

4. Importe la configuración del grupo de servidores 1 de vuelta en el nodo 2012R2-A.

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject

5. Propague la configuración recién importada en todo el grupo de servidores, de modo que los servidores tengan una configuración uniforme después de la importación.

Escenario 2: Hacer una copia de seguridad de una configuración existente desde el grupo de servidores 1 y usarla para crear un nuevo grupo de servidores en una instalación diferente predeterminada de fábrica. A continuación, se pueden agregar nuevos servidores miembros de grupo al nuevo servidor principal.

Se crea el grupo de servidores 2, que contiene dos servidores nuevos: 2012R2-C y 2012R2-D. La configuración del grupo de servidores 2 se basará en la configuración de una implementación existente, la del grupo de servidores 1, que también contiene dos servidores: 2012R2-A y 2012R2-B. El clúster CitrixClusterMembership contenido en el archivo de copia de seguridad no se usa al crear un nuevo grupo de servidores. Siempre se hace una copia de seguridad del clúster CitrixClusterMembership actual y luego se restaura después de una importación correcta. Al crear una implementación nueva usando una configuración importada, el grupo de seguridad de CitrixClusterMembership solo contiene el servidor que recibe la importación hasta que se agregan servidores adicionales al grupo. El grupo de servidores 2 es una nueva implementación que va a coexistir con el grupo de servidores 1. Especifique el parámetro -HostBaseURL. El grupo de servidores 2 se creará usando una instalación de StoreFront limpia que tiene los valores predeterminados de fábrica.

1. Exporte la configuración del grupo de servidores 1 desde 2012R2-A, que es el servidor principal utilizado para administrar todo el grupo de servidores.

2. Importe la configuración del grupo de servidores 1 en el nodo 2012R2-C, que será el servidor principal utilizado para administrar todo el grupo de servidores 2 recién creado.

Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -HostBaseURL "https://grupoDeServidores2.ejemplo.com"

3. Incorpore servidores adicionales que formarán parte de la nueva implementación del grupo de servidores 2. La propagación de la configuración recién importada desde el grupo de servidores 1 a todos los nuevos miembros del grupo de

servidores 2 es automática, ya que esto forma parte del proceso normal de incorporación de nuevos servidores a un grupo.

Escenario 3: Hacer una copia de seguridad de una configuración existente desde el grupo de servidores 1 y usarla para sobrescribir la configuración existente del grupo de servidores 2.

El grupo de servidores 1 y el grupo de servidores 2 ya existen, y están en dos centros de datos distintos. Se han hecho muchos cambios en la configuración de StoreFront del grupo de servidores 1 y deben aplicarse al grupo de servidores 2 situado en el otro centro de datos. Estos cambios pueden transferirse desde el grupo de servidores 1 al grupo de servidores 2. No use la información de **CitrixClusterMembership** contenida en el archivo de copia de seguridad en el grupo de servidores 2. Especifique el parámetro **-HostBaseURL** durante la importación, ya que la URL base de host del grupo de servidores 2 no debe cambiarse por el mismo FQDN que usa el grupo de servidores 1. El grupo de servidores 2 es una implementación existente.

1. Exporte la configuración del grupo de servidores 1 desde 2012R2-A, que es el servidor principal utilizado para administrar todo el grupo de servidores.

2. Importe la configuración del grupo de servidores 1 en el nodo 2012R2-C que tiene la instalación predeterminada de fábrica, y será el servidor principal utilizado para el grupo de servidores 2.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject -
HostBaseURL "https://grupoDeServidores2.ejemplo.com"
```

StoreFront SDK

Aug 14, 2017

Citrix StoreFront proporciona un SDK basado en una serie de módulos de Microsoft Windows PowerShell 3.0. Con el SDK, se pueden realizar las mismas tareas que se llevan a cabo con la consola MMC de StoreFront, junto con otras tareas que no se pueden realizar con la consola.

Para la referencia del SDK, consulte SDK de StoreFront.

Diferencias principales entre el SDK de StoreFront 3.0 y el SDK de StoreFront actual

- **Ejemplos de SDK de alto nivel:** Esta versión proporciona scripts de SDK de alto nivel que permiten automatizar las implementaciones de StoreFront de manera rápida y sencilla. Puede personalizar los ejemplos de alto nivel para que se ajuste a sus requisitos concretos, o puede crear una nueva implementación simplemente ejecutando un script.
- **Nuevo SDK de bajo nivel:** Citrix proporciona un SDK documentado de bajo nivel para StoreFront, que le permite configurar las implementaciones, incluidas las tiendas, los métodos de autenticación, los sitios de Citrix Receiver para Web y Unified Citrix Receiver, así como el acceso remoto a través de NetScaler Gateway.
- **Compatibilidad con versiones anteriores:** StoreFront 3.6 todavía contiene las API de StoreFront 3.0 y versiones anteriores, lo que facilita la transición gradual desde los scripts existentes a los del nuevo SDK.

Important

La compatibilidad con versiones anteriores con StoreFront 3.0 se ha mantenido siempre que ha sido posible y viable. Sin embargo, Citrix recomienda que, al escribir nuevos scripts, se usen los nuevos módulos **Citrix.StoreFront.***, ya que el SDK de StoreFront 3.0 se considera obsoleto y será eliminado en el futuro.

Uso de SDK

El SDK se compone de una serie de complementos de PowerShell que el asistente de instalación instala automáticamente cuando se instalan y se configuran varios componentes de StoreFront.

Para acceder a los cmdlets y ejecutarlos:

1. Inicie un shell en PowerShell 3.0.
   Debe ejecutar el shell o el script usando una cuenta miembro del grupo de administradores locales en el servidor StoreFront.

2. Para utilizar los cmdlets del SDK en scripts, configure la directiva de ejecución en PowerShell.
   Para obtener más información acerca de la directiva de ejecución de PowerShell, consulte la documentación de Microsoft.

3. Agregue los módulos que necesite al entorno de PowerShell con el comando **Add -Module** en la consola de Windows PowerShell. Por ejemplo, escriba:
   ```
   Import-Module Citrix.StoreFront
   ```
   Para importar todos los cmdlets, escriba:

```
Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront") } | Import-Module
```

Después de realizar la importación, tendrá acceso a los cmdlets y a la ayuda asociada.

Introducción a SDK

Para crear un script, siga los siguientes pasos:

1. Tome uno de los ejemplos del SDK instalado por StoreFront en la carpeta **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples**.
2. Para ayudarle a personalizar su propio script, consulte el script de ejemplo para comprender lo que hace cada parte. Para obtener más información, consulte el caso de uso de ejemplo que describe con más detalle las acciones del script.
3. Adapte los scripts de ejemplo para convertirlos en scripts más útiles para su consumo. Para hacerlo:
   - Use PowerShell ISE o una herramienta similar para editar el script.
   - Utilice variables para asignarles valores que se van a volver a utilizar o modificar.
   - Elimine los comandos que no sean necesarios.
   - Observe que los cmdlets de StoreFront se pueden identificar por el prefijo STF.
   - Use el cmdlet Get-Help con el nombre de un cmdlet y el parámetro -Full para obtener más información acerca de un comando en concreto.

Ejemplos

Nota: Al crear un script, para asegurarse de obtener siempre las mejoras y revisiones más recientes, Citrix recomienda seguir el procedimiento descrito en este tema en lugar de copiar y pegar el script de ejemplo.

Ejemplos	Descripción
	Script: Crea una implementación simple de StoreFront con un controlador configurado con un único servidor XenDesktop.
	Script: Se basa en el script anterior y añade acceso remoto a la implementación.
	Script: Se basa en el script anterior y añade puertas de enlace preferidas óptimas para mejorar la experiencia del usuario.
	Script: Crea una implementación simple configurada con un sitio de Desktop Appliance.

Ejemplo: Crear una implementación simple

El siguiente ejemplo muestra cómo crear una implementación simple configurada con un Controller de XenDesktop.

Antes de comenzar, compruebe que sigue los pasos detallados en Introducción al SDK. Este ejemplo se puede personalizar usando los métodos descritos para generar un script que automatice la implementación de StoreFront.

Nota: Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script

Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de 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"
)

# Importar módulos de StoreFront Requerido para versiones de PowerShell anteriores a la 3.0 que no respaldan la carga automática
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Authentication
Import-Module Citrix.StoreFront.WebReceiver
```

- Automatiza la ruta virtual de los servicios de autenticación y Citrix Receiver para Web basándose en la ruta **$StoreVirtualPath** proporcionada.

```
# Determinar la ruta virtual de autenticación y Receiver para usar en función de la tienda

$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"

$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
```

- Crea una nueva implementación si todavía no hay ninguna, como preparación para agregar los servicios de StoreFront. **-Confirm:$false** suprime el requisito de confirmar que la implementación puede continuar.

```
# Determine si la implementación ya existe

$existingDeployment = Get-STFDeployment

if(-not $existingDeployment)

{

   # Instalar los componentes de StoreFront necesarios

   Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -Confirm:$false

}

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)

{

   # La implementación existe y está configurada para la URL de base del host deseado

   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."

}
```

- Crea un nuevo servicio de autenticación si todavía no hay ninguno en la ruta virtual especificada El método de autenticación predeterminado de nombre de usuario y contraseña está habilitado.

```
# Determinar si existe el servicio de autenticación en la ruta virtual especificada

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

if(-not $authentication)

{

   # Agregar un servicio de autenticación usando la ruta IIS de la tienda con Auth

   $authentication = Add-STFAuthenticationService $authenticationVirtualPath
```



```
}

else

{

   Write-Output "An Authentication service already exists at the specified virtual path and will be used."

}
```

- Crea un nuevo servicio de autenticación si todavía no hay ninguno en la ruta virtual especificada El método de autenticación predeterminado de nombre de usuario y contraseña está habilitado.

```
# Determinar si existe el servicio de autenticación en la ruta virtual especificada

$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath

if(-not $authentication)

{

   # Agregar un servicio de autenticación usando la ruta IIS de la tienda con Auth

   $authentication = Add-STFAuthenticationService $authenticationVirtualPath

}

else

{

   Write-Output "An Authentication service already exists at the specified virtual path and will be used."

}
```

- Crea un nuevo servicio de tienda configurado con un Controller de XenDesktop con los servidores en la matriz **$XenDesktopServers** en la ruta virtual especificada, si todavía no existe ninguna.

```
# Determinar si existe el servicio de tienda en la ruta virtual especificada

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

if(-not $store)

{

# Agregar una tienda que use el nuevo servicio de autenticación configurado para publicar recursos de los servidores suministrados

$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."

    # Obtener la cantidad de comunidades configuradas en la tienda

    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count

    # Añadir la comunidad a la tienda con un nombre único

    Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port `

        -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- Agrega un servicio de Citrix Receiver para Web en la ruta virtual de IIS especificada para obtener acceso a las aplicaciones publicadas en la tienda creada anteriormente.

```
# Determinar si existe el servicio de Receiver en la ruta virtual especificada

$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath

if(-not $receiver)

{

    # Agregar un sitio de Receiver para Web para que los usuarios puedan acceder a las aplicaciones y escritorios en la tienda

    $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."

}
```

- Habilita los servicios XenApp para la tienda de modo que los clientes Citrix Receiver de versiones anteriores puedan conectarse a las aplicaciones publicadas.

```
# Determinar si PNA está configurado para el servicio de tienda

$storePnaSettings = Get-STFStorePna -StoreService $store

if(-not $storePnaSettings.PnaEnabled)
```



```
{
  # Habilitar los servicios XenApp la tienda y hacerlo parámetro predeterminado para este servidor
  Enable-STFStorePna -StoreService $store -AllowUserPasswordChange -DefaultPnaService
}
```

Ejemplo: Crear una implementación para acceso remoto

El siguiente ejemplo se basa en el script anterior y agrega una implementación de acceso remoto.

Antes de comenzar, compruebe que sigue los pasos detallados en Introducción al SDK. Este ejemplo se puede personalizar usando los métodos descritos para generar un script que automatice la implementación de StoreFront.

Nota: Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script

Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de 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

# Cualquier fallo hace terminar la operación.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Importar módulos de StoreFront Requerido para versiones de PowerShell anteriores a la 3.0 que no respaldan la carga automática
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
```

- Cree una implementación de StoreFront de acceso interno ejecutando los scripts de los ejemplos anteriores. La implementación básica se ampliará para dar respaldo al acceso remoto.

```
# Crear una implementación sencilla invocando el ejemplo SimpleDeployment
$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
```

- Obtiene los servicios creados en la implementación sencilla porque tienen que actualizarse para dar respaldo al escenario

de acceso remoto.

```
# Determinar si sitios de autenticación y Receiver en función de la tienda

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$authentication = Get-STFAuthenticationService -StoreService $store

$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- Habilita CitrixAGBasic en el servicio de Citrix Receiver para Web, requerido para el acceso remoto a través de NetScaler Gateway. Obtenga el método de autenticación ExplicitForms y CitrixAGBassic de Citrix Receiver para Web de los protocolos respaldados.

```
# Obtener el método de autenticación ExplicitForms y CitrixAGBassic de Citrix Receiver para Web de los protocolos respaldados

# Incluido con fines de demostración, porque se puede usar el nombre del protocolo si se conoce

$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable | Where-Object { $_ -match "Explicit" -or $_ -match "CitrixAG" }

# Habilitar CitrixAGBasic en Receiver para Web (requerido para el acceso remoto)

Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods $receiverMethods
```

- Habilita CitrixAGBasic en el servicio de autenticación. Esto es necesario para el acceso remoto.

```
# Obtener el método de autenticación CitrixAGBasic de los protocolos instalados.

# Incluido con fines de demostración, porque se puede usar el nombre del protocolo si se conoce

$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object { $_ -match "CitrixAGBasic" }

# Habilitar CitrixAGBasic en el servicio de autenticación (requerido para el acceso remoto)

Enable-STFAuthenticationServiceProtocol -AuthenticationService $authentication -Name $citrixAGBasic
```

- Agrega una nueva puerta de enlace de acceso remoto, agregando la dirección IP de subred optativa y registrándola con la tienda a la que se va a obtener acceso de forma remota.

```
# Agregar una nueva puerta de enlace utilizad para acceder a la nueva tienda de forma remota

Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version Version10_0_69_4 -GatewayUrl $GatewayUrl '

-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls $GatewaySTAUrls

# Obtener la nueva puerta de enlace de la configuración (Add-STFRoamingGateway devolverá la nueva puerta de enlace si se incluye el parámetro - PassThru)

$gateway = Get-STFRoamingGateway -Name $GatewayName

# Si se suministró la subred de la puerta de enlace, configúrela en el objeto de puerta de enlace
```

```
if($GatewaySubnetIP)

{

   Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress $GatewaySubnetIP

}

# Registre la puerta de enlace en la nueva tienda

Register-STFStoreGateway -Gateway $gateway -StoreService $store -DefaultGateway
```

Ejemplo: Crear una implementación para acceso remoto con una puerta de enlace óptima

El siguiente ejemplo se basa en el script anterior y agrega una implementación de acceso remoto con puerta de enlace de inicio óptima.

Antes de comenzar, asegúrese de seguir los pasos detallados en Introducción a SDK. Este ejemplo se puede personalizar usando los métodos descritos para generar un script que automatice la implementación de StoreFront.

Nota: Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script

Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de 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

# Cualquier fallo hace terminar la operación.

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

# Importar módulos de StoreFront Requerido para versiones de PowerShell anteriores a la 3.0 que no respaldan la carga automática

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- Llama al script de implementación de acceso remoto para configurar la implementación básica y agregarle el acceso remoto.

```
# Crear una implementación para acceso remoto

$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
```

- Agrega la preferencia de puerta de enlace de inicio óptima y la obtiene de las puertas de enlace configuradas.

```
# Agregue una nueva puerta de enlace utilizada para el acceso remoto HDX a escritorios y aplicaciones

$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType UsedForHDXOnly -GatewayUrl
$OptimalGatewayUrl -SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
```

- Obtiene el servicio de la tienda para usar la puerta de enlace óptima, registrarla y asignarla a inicios desde una comunidad especificada.

```
# Obtener la tienda configurada por SimpleDeployment.ps1

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Registrar la puerta de enlace con la nueva tienda para inicarla con todas las comunidades (actualmente solo una)

$farmNames = @($store.FarmsConfiguration.Farms | foreach { $_.FarmName })

Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService $store -FarmName $farmNames
```

Ejemplo: Crear una implementación con un sitio de Desktop Appliance

El siguiente ejemplo se basa en el ejemplo de implementación simple y le agrega un sitio de Desktop Appliance.

Antes de comenzar, asegúrese de seguir los pasos detallados en Introducción a SDK. Este ejemplo se puede personalizar usando los métodos descritos para generar un script que automatice la implementación de StoreFront.

Nota: Para asegurarse de que siempre obtiene las últimas mejoras y revisiones, Citrix recomienda seguir el procedimiento descrito en este documento en lugar de copiar y pegar el script de ejemplo.

Entender el script

Esta sección explica qué hace cada parte del script generado por StoreFront. Esto le ayudará con la personalización de su propio script.

- Establece los requisitos para la gestión de errores e importa los módulos de StoreFront necesarios. La importación no es necesaria en versiones más nuevas de 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

# Cualquier fallo hace terminar la operación.

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

# Importar módulos de StoreFront Requerido para versiones de PowerShell anteriores a la 3.0 que no respaldan la carga automática

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- Automatizar la ruta de un dispositivo de escritorio basada en la de $StoreVirtualPath.

```
$desktopApplianceVirtualPath = "$($StoreIISPath.TrimEnd('/'))Appliance"
```

- Llama a un script de implementación simple para configurar una implementación predeterminada con los servicios requeridos.

```
# Crear una implementación para acceso remoto

$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
```

- Obtiene el servicio de tienda para usarlo con el sitio de Desktop Appliance. Use el cmdlet **Add-STFDesktopApplianceService** para agregar el nuevo sitio con autenticación explícita de nombre de usuario y contraseña y hacerlo un sitio multiescritorio.

```
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Crear un nuevo sitio de Desktop Appliance con los escritorios publicados por el servicio de tienda

Add-STFDesktopApplianceService -VirtualPath $desktopApplianceVirtualPath -StoreService $store -EnableExplicit
```

Ejemplo: Intercambio de metadatos entre el proveedor de identidades y el proveedor de servicios (StoreFront) para la autenticación SAML

La autenticación SAML se puede configurar en la consola de administración de StoreFront (consulte Configuración del

servicio de autenticación) o usando los cmdlets de PowerShell siguientes: Export-STFSamlEncryptionCertificate, Export-STFSamlSigningCertificate, Import-STFSamlEncryptionCertificate, Import-STFSamlSigningCertificate, New-STFSamlEncryptionCertificate, New-STFSamlIdPCertificate, New-STFSamlSigningCertificate.

Puede usar el cmdlet **Update-STFSamlIdPFromMetadata**, para intercambiar metadatos (identificadores, certificados, dispositivos de punto final y otro tipo de configuración) entre el proveedor de identidades y el proveedor de servicios, que es StoreFront en este caso.

Para una tienda de StoreFront, llamado "Store", con su servicio de autenticación dedicado, el punto final de metadatos será:

https:///Citrix/StoreAuth/SamlForms/ServiceProvider/Metadata

Si el proveedor de identidades es compatible con la importación de metadatos, puede apuntar a la URL anterior. **Nota**: Esto debe llevarse a cabo a través de HTTPS.

Para que StoreFront consuma los metadatos de un proveedor de identidades, se puede utilizar el siguiente comando de PowerShell:

comando COPIAR

```
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
```

Ejemplo: Listar los metadatos y los puntos finales de ACS para una tienda especificada para la autenticación SAML

Se puede utilizar el siguiente script para crear una lista de los puntos finales ACS (Assertion Consumer Service) y los metadatos para una tienda específicada.

comando COPIAR

```
# 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"
```

Ejemplo de resultado

```
comando                                                    COPIAR
```

```
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
```

Solución de problemas de StoreFront

Aug 14, 2017

Cuando se instala o desinstala StoreFront, el instalador de StoreFront crea los siguientes archivos de registros en el directorio C:\Windows\Temp\. Los nombres de archivo reflejan los componentes que los han creado e incluyen marcas de tiempo.

- Citrix-DeliveryServicesRoleManager-*.log: creado cuando StoreFront se instala de forma interactiva.
- Citrix-DeliveryServicesSetupConsole-*.log: creado cuando StoreFront se instala de forma silenciosa, y cuando se desinstala, ya sea de forma interactiva o silenciosa.
- CitrixMsi-CitrixStoreFront-x64-*.log: creado cuando StoreFront se instala o desinstala, ya sea de forma interactiva o silenciosa.

StoreFront admite el registro de sucesos de Windows para el servicio de autenticación, las tiendas y los sitios de Receiver para Web. Todos los eventos que se generan se escriben en el registro de aplicaciones de StoreFront, que se puede ver a través de Visor de eventos ya sea en Registros de aplicaciones y servicios > Citrix Delivery Services o mediante Registros de Windows > Aplicación. Para controlar la cantidad de entradas de registro duplicadas de un solo suceso, modifique los archivos de configuración del servicio de autenticación, de las tiendas y de los sitios de Receiver para Web.

La consola de administración de Citrix StoreFront registra automáticamente la información de seguimiento. De forma predeterminada, el seguimiento de otras operaciones está inhabilitado y se debe habilitar de forma manual. Los registros creados mediante comandos de Windows PowerShell se almacenan en el directorio \Admin\logs\ de la instalación de StoreFront. Por lo general, su ubicación típica es C:\Archivos de programa\Citrix\Receiver StoreFront\. Los nombres de los archivos de registro contienen acciones y sujetos de comandos, además de marcas de tiempo que se pueden usar para distinguir las secuencias de comandos.

Importante: En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

Para configurar la limitación de registros

1. Utilice un editor de texto para abrir el archivo web.config del servicio de autenticación, la tienda o el sitio de Receiver para Web, que normalmente se encuentra en los directorios C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\ y C:\inetpub\wwwroot\Citrix\storenameWeb\, respectivamente, donde storename es el nombre que se especificó para la tienda durante su creación.
2. Localice el siguiente elemento en el archivo.
   De forma predeterminada, StoreFront se configura para limitar la cantidad de entradas de registro duplicadas a 10 por minuto.

3. Cambie el valor del atributo duplicateInterval para definir el período en el formato de horas, minutos y segundos durante el que se controlarán las entradas de registros duplicadas. Utilice el atributo duplicateLimit para definir la cantidad de entradas duplicadas que se deben registrar en el intervalo especificado para iniciar la limitación de registros.

Cuando se inicie la limitación de registros, se registrará un mensaje de advertencia para indicar que se omitirán las entradas de registro posteriores que sean idénticas. Después de este límite de tiempo, se reanuda el registro normal y se registra un mensaje informativo que indica que las entradas de registro duplicadas ya no se omitirán.

Para habilitar el seguimiento

Advertencia: Las consolas de StoreFront y PowerShell no pueden estar abiertas a la vez. Cierre siempre la consola de administración de StoreFront antes de usar la consola de PowerShell para administrar la configuración de StoreFront. Asimismo, cierre todas las instancias de PowerShell antes de abrir la consola de StoreFront.

1. Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell y, en el símbolo del sistema, escriba los siguientes comandos para reiniciar el servidor y habilitar el seguimiento.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands Set-DSTraceLevel -All -TraceLevel Verbose
   Los valores permitidos para -TraceLevel son, en orden creciente de detalle de seguimiento: Off, Error, Warning, Info, Verbose.
   StoreFront captura automáticamente los mensajes de error de seguimiento. Debido a la gran cantidad de datos que se puede llegar a generar, el seguimiento puede afectar de manera significativa el rendimiento de StoreFront, por lo que se recomienda que los niveles Info o Verbose no se utilicen a menos que sean necesarios para la solución de problemas.

   Los argumentos opcionales para el cmdlet Set-DSTraceLevel son:
   -FileCount: Especifica la cantidad de archivos de seguimiento (predeterminado = 3)
   -FileSizeKb: Especifica el tamaño máximo de cada archivo de seguimiento (predeterminado = 1000)
   -ConfigFile : Una alternativa a -All que permite la actualización de un solo archivo de configuración, en lugar de todos. Por ejemplo, un valor de c:\inetpub\wwwroot\Citrix\\web.config para -ConfigFile, establecería un seguimiento para la tienda llamado .

2. Para inhabilitar el seguimiento, escriba los siguientes comandos y reinicie el servidor.
   Add-PSSnapin Citrix.DeliveryServices.Framework.Commands Set-DSTraceLevel -All -TraceLevel Off

Cuando se habilita el seguimiento, la información de seguimiento se escribe en el directorio de instalación \Admin\Trace\ de StoreFront, ubicado en C:\Archivos de programa\Citrix\Receiver StoreFront\.