CITRIX

StoreFront 1912

Contents

StoreFront 1912

January 31, 2020

StoreFront 1912 es la versión actual (Current Release) más reciente de StoreFront. Esta documentación refleja las funciones y las configuraciones de esta versión.

StoreFront es un intuitivo almacén de aplicaciones de empresa que combina aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops en un solo almacén. StoreFront es el componente fundamental de Citrix Virtual Apps and Desktops que se puede utilizar con otras versiones de Virtual Apps and Desktops.

Los usuarios pueden trabajar con la aplicación Citrix Workspace o las versiones compatibles de Citrix Receiver para acceder a los almacenes de StoreFront. Si una versión específica se comporta de manera diferente o el texto de la interfaz de usuario hace referencia a ambas, se le indica. De lo contrario, la documentación se refiere a la "aplicación Citrix Workspace".

Versiones anteriores

Para ver la documentación sobre las versiones anteriores, consulte:

- StoreFront 1909
- StoreFront 1906
- StoreFront 1903
- StoreFront 1811
- StoreFront 3.16
- StoreFront 3.12
- StoreFront 3.0
- Versiones anteriores de StoreFront

La estrategia de ciclos de vida para las versiones Current Release (CR) y las versiones Long Term Service (LTSR) de Citrix Virtual Apps and Desktops se describe en Hitos del ciclo de vida. En CTX200356 se ofrece información adicional sobre el ciclo de vida de StoreFront.

> **Nota:**
>
> No se admiten actualizaciones a la versión Current Release de StoreFront más reciente a partir de versiones anteriores no admitidas. Si utiliza versiones Current Release, debe comprobar que está en una versión compatible de StoreFront Current Release en todo momento.

Novedades

January 31, 2020

StoreFront 1912

StoreFront 1912 incluye las siguientes funciones nuevas. Para ver información sobre las correcciones de errores, consulte Problemas resueltos.

La compatibilidad con controladores de protocolo StoreFront ahora incluye dispositivos Chrome con la aplicación Workspace para Android

Cuando los usuarios de dispositivos Chrome abren un sitio de Citrix Receiver para Web y la aplicación Citrix Workspace para Android 1912 o una versión posterior está instalada, el explorador abre automáticamente los archivos ICA con dicha aplicación al iniciarse.

Ahora, el flujo de trabajo de detección de clientes para Android, que determina si la aplicación Citrix Workspace para Android está instalada, es idéntico al de los clientes de la aplicación Citrix Workspace para Windows y Citrix Workspace para MAC cuando se utiliza el explorador Chrome en dispositivos Chrome. En versiones anteriores, los usuarios de dispositivos Chrome tenían que, en primer lugar, abrir manualmente un archivo ICA descargado.

Compatibilidad con directivas de protección de aplicaciones

StoreFront 1912 es compatible con directivas de protección de aplicaciones para mejorar la seguridad cuando otros componentes de Citrix, como la aplicación Citrix Workspace y los Delivery Controllers de Citrix Virtual Apps and Desktops, también lo son. Las directivas de protección de aplicaciones se establecen en el nivel de grupo de entrega, y Citrix Virtual Apps and Desktops determina si se utilizan las directivas de protección de aplicaciones. Es necesario habilitar manualmente la función de protección de aplicaciones en StoreFront. Cuando StoreFront recibe solicitudes que contienen el encabezado HTTP X-Citrix-AppProtection-Capable desde una aplicación de Citrix Workspace compatible con directivas de protección de aplicaciones, StoreFront envía automáticamente una etiqueta de acceso inteligente a Citrix Virtual Apps and Desktops que indica que admite directivas de protección de aplicaciones. Para obtener información detallada sobre cómo configurar grupos de entrega con directivas de protección de aplicaciones, consulte Protección de aplicaciones.

Para habilitar la protección de aplicaciones en un servidor StoreFront, ejecute el siguiente comando de PowerShell en el servidor StoreFront: `Add-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control" -IsEnabled $True`. (En una implementación

de StoreFront de varios servidores, debe propagar manualmente estos cambios a todos los demás servidores del grupo; consulte Propagar cambios locales en un grupo de servidores).

Para comprobar que la funcionalidad está habilitada en un servidor StoreFront, utilice el siguiente comando de PowerShell:
`Get-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control`.

Los sitios de Desktop Appliance ya no son compatibles

La compatibilidad con StoreFront para que los usuarios accedan a escritorios en sitios de Desktop Appliance se anunció como retirada en Citrix Virtual Apps and Desktops 7 1811. En esta versión, los sitios de Desktop Appliance ya no son compatibles, y se recomienda utilizar la aplicación Desktop Lock de Citrix Workspace para todos los casos de uso que no estén unidos a un dominio.

> **Advertencia:**
>
> Al actualizar a StoreFront 1912, todos los sitios de Desktop Appliance de la implementación se quitan automáticamente. Consulte Actualizar StoreFront.

StoreFront PowerShell SDK

PowerShell SDK de StoreFront se ha vuelto a publicar como versión 1912. Ya no puede crear ni administrar sitios de Desktop Appliance mediante PowerShell.

Problemas resueltos

January 6, 2020

Se han solucionado los problemas siguientes desde la versión 1909:

- En las instancias locales de StoreFront no se pueden agregar enlaces web para iniciar Gateway en MMC. [WSP-4368]
- LCM-6351: Las claves del Registro antiguas de CitrixPrivilegedService_x64.msi no se quitaron después de actualizar la versión de DDC. [WSP-4785]
- Si VMware VMTools v10.3.x está instalado en el servidor de StoreFront al intentar actualizar la versión de StoreFront a la 1906 mediante el metainstalador de Citrix Virtual Apps and Desktops 7 1906, se produce un error en la actualización. La versión de StoreFront se actualiza correctamente con el instalador independiente de StoreFront 1906, pero StoreFront 1906 no se agrega a la lista Agregar o quitar programas de Windows. [WSP-4895]

- La personalización para truncar nombres de aplicación largos ya no funciona en la IU de X1.1 Purple. [WSP-4899]
- Es posible que las actualizaciones que incluyen desde 2.6, 3.0.1, 3.5 y 3.8 en su historial de actualizaciones a 3.12 CU* o una versión posterior fallen si el servicio KCD se halla en estado Detenido. [WSP-5160]
- Actualice `http://downloadplugins.citrix.com` para entregar la aplicación Citrix Workspace en lugar de Citrix Receivers al final de su vida útil. [WSP-5303]

Problemas conocidos

January 6, 2020

Estos son los problemas conocidos de esta versión.

- La propagación de la suscripción entre los miembros de un grupo de servidores de StoreFront falla cuando TLS 1.0 está inhabilitado en Windows y Windows Server usa el servidor .NET Framework 4.5. De forma predeterminada, .NET Framework 4.5 usa solo TLS 1.0. Una solución temporal para este problema es actualizar .NET Framework en el servidor a la versión 4.7 o posterior (que usa TLS 1.2 de manera predeterminada). [STF-2413]
- Existe un problema conocido de terceros con la autenticación de tarjeta inteligente y Microsoft Edge. Como solución temporal, use Internet Explorer. [DNA-47809]
- 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, DNA-22561]
- Cuando StoreFront está instalado en Windows Server 2012 R2, es posible que no se registre con Citrix Analytics Service (CAS). Esto sucede cuando todavía no están instalados los componentes de software del runtime de C++. El instalador independiente de StoreFront no instala estos componentes. Una solución sencilla consiste en instalar el runtime de C++ antes o después de instalar StoreFront. [WSP-4412]

Avisos de legales de terceros

January 6, 2020

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

Avisos legales de terceros de StoreFront (descarga en PDF)

Requisitos del sistema

January 31, 2020

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 del almacén 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.

> **Nota:**
>
> No se admite la actualización a la versión más reciente desde una versión antigua que esté en el ciclo Fin de vida. Para obtener más información, consulte CTX200356.

Después de las pruebas pertinentes, Citrix admite las instalaciones de StoreFront en las siguientes plataformas:

- Windows Server 2019 ediciones Datacenter y Standard
- Windows Server 2016 ediciones Datacenter y Standard
- Windows Server 2012 R2 ediciones Datacenter y Standard

No se admite la actualización de versiones de los sistemas operativos en un servidor con StoreFront. 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 admiten los grupos de servidores de StoreFront que contengan combinaciones de versiones de sistema operativo y configuraciones regionales. Los grupos de servidores de StoreFront pueden contener hasta seis servidores. Sin embargo, desde el punto de vista de la capacidad basada en simulaciones, los grupos de servidores con más de tres servidores no suponen ninguna ventaja. Lo ideal sería que todos los servidores de un grupo de servidores residan en la misma ubicación (centro de datos, zona de disponibilidad), pero los grupos de servidores pueden abarcar varias ubicaciones dentro de la misma región siempre que los vínculos entre los servidores del grupo cumplan criterios mínimos de latencia. Consulte Escalabilidad.

Antes de poder instalar StoreFront, Windows PowerShell (versión 4.0 o una posterior) y Microsoft Management Console (versión 3.0 o una posterior) deben estar instalados en el servidor web. Son componentes predeterminados de Windows Server.

El instalador de StoreFront comprueba que los siguientes requisitos previos estén instalados y habilitados antes de instalar StoreFront. De forma predeterminada, el sistema operativo proporciona estos requisitos previos como paquetes de funciones. Si el instalador de StoreFront detecta requisitos previos que faltan o que están inhabilitados, los instala y los activa automáticamente:

- Microsoft .NET Framework (versión 4.5.1 o una posterior)
- Microsoft ASP.NET (versión 4.5 o una posterior)
- Runtime de Microsoft Visual C++ VC141 x64
- Microsoft Internet Information Services (IIS)

  IIS se agrega mediante el rol de servidor web "Windows Server", cuya versión depende del sistema operativo elegido. Como referencia, el instalador de StoreFront agrega estos roles de IIS:

  - Web-Static-Content
  - Web-Default-Doc
  - Web-Http-Errors
  - Web-Http-Redirect
  - Web-Http-Logging
  - Web-Mgmt-Console
  - Web-Scripting-Tools
  - Web-Windows-Auth
  - Web-Basic-Auth
  - Web-AppInit
  - Web-Asp-Net45
  - Net-Wcf-Tcp-PortSharing45

  La ruta relativa a StoreFront en IIS debe ser la misma para todos los servidores de un grupo de servidores.

StoreFront utiliza los siguientes puertos para comunicarse. 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 de StoreFront y, por ello, debe ser accesible.
- Para las comunicaciones entre los servidores de 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.

- La aplicación Citrix Workspace para HTML5 y otras versiones admitidas de Citrix Receiver y de la aplicación Citrix Workspace utilizan 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.

Almacenar datos de suscripción mediante Microsoft SQL Server

Usted puede, opcionalmente, Almacenar datos de suscripción mediante Microsoft SQL Server. StoreFront admite las mismas versiones de Microsoft SQL Server para esto que Citrix Virtual Apps and Desktops para bases de datos. En los requisitos del sistema de Citrix Virtual Apps and Desktops, consulte Bases de datos.

Requisitos de infraestructura

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

Requisitos del servidor Citrix

Los almacenes de StoreFront combinan escritorios y aplicaciones de los siguientes productos.

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

* Para obtener más información sobre el uso de esta versión actual (CR) en un entorno de servicio a largo plazo (LTSR) y otras preguntas frecuentes, consulte el artículo de Knowledge Center.

Requisitos de Citrix Gateway

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

- Citrix Gateway 13.0

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

Requisitos de la aplicación Citrix Workspace para HTML5

Tenga en cuenta los siguientes requisitos adicionales para permitir que los usuarios accedan a escritorios y aplicaciones a través de la aplicación Citrix Workspace para HTML5 activa en los sitios de Receiver para Web.

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

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

> **Nota:**
>
> La aplicación Citrix Workspace para HTML5 solo inicia escritorios y aplicaciones mediante conexiones de red internas cuando se han configurado conexiones seguras a los VDA que alojan esos recursos. No puede usar conexiones HTTP con los VDA que alojan las aplicaciones y los escritorios.

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

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

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

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906

- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp y XenDesktop 7.15 LTSR
- XenApp y XenDesktop 7.6 LTSR

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 la aplicación Citrix Workspace pueden acceder a los almacenes a través de aplicación Citrix Workspace, o pueden utilizar un explorador web para iniciar sesión en el sitio de Citrix Receiver para Web del almacén. Para los usuarios que no pueden instalar la aplicación Citrix Workspace, 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 la aplicación Citrix Workspace para HTML5 en los sitios de Citrix Receiver para Web.

Los usuarios con equipos reasignados que cuentan con Citrix Desktop Lock, junto con clientes Citrix anteriores que no se pueden actualizar, deben conectarse a través de la URL de XenApp Services para el almacén.

Para entregar a los usuarios secuencias de Microsoft Application Virtualization (App-V), también se necesita una versión compatible de Microsoft Application Virtualization Desktop Client. Para obtener más información, consulte Administrar 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.

Usar la aplicación Citrix Workspace para acceder a los almacenes de StoreFront

Puede utilizar todas las versiones admitidas de la aplicación Citrix Workspace para acceder a los almacenes de StoreFront mediante conexiones desde la red interna y a través de Citrix Gateway. Para conocer las fechas de los ciclos de vida de la aplicación Citrix Workspace y de Citrix Receiver, consulte https://www.citrix.com/support/product-lifecycle/milestones/receiver.html.

Puede conectarse a los almacenes de StoreFront a través de Citrix Gateway mediante el plug-in de Citrix Gateway, el proxy ICA o la VPN sin cliente (CVPN). Consulte Experiencia de usuario unificada.

Acceder a almacenes a través de los sitios de Citrix Receiver para Web

Para acceder a los sitios de Citrix Receiver para Web mediante conexiones de la red interna y a través de Citrix Gateway, utilice la versión más reciente de los siguientes exploradores:

En Windows

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

En Mac

- Safari
- Google Chrome
- Mozilla Firefox

En Linux

- Google Chrome
- Mozilla Firefox

Es posible establecer conexiones a través de Citrix Gateway mediante el plug-in de Citrix Gateway, el proxy ICA o la red VPN sin cliente (cVPN). Además, se necesitan versiones específicas de Citrix Gateway para habilitar las conexiones desde fuera de la red corporativa. Para obtener más información, consulte Requisitos de infraestructura.

Iniciar recursos a través de sitios de Citrix Receiver para Web

Los sitios de Citrix Receiver para Web admiten el inicio de recursos a través de una aplicación Citrix Workspace instalada de forma nativa o a través de la aplicación Citrix Workspace para HTML5. Todos los exploradores indicados anteriormente son compatibles con HTML5 y admiten el inicio de recursos en HTML5. Según su configuración de Receiver para Web, los usuarios finales pueden elegir cualquiera de los dos métodos de inicio de recursos.

Acceder a almacenes a través de direcciones URL de XenApp Services

Puede utilizar las direcciones URL de XenApp Services para acceder a los almacenes de StoreFront con una funcionalidad reducida. Las direcciones URL de XenApp Services ofrecen retrocompatibilidad con versiones anteriores para las conexiones realizadas por Citrix Receiver 3.4 Enterprise y clientes más antiguos que solo admiten conexiones a través de PNAgent. En caso de disponibilidad, es posible establecer conexiones a través de Citrix Gateway mediante el plug-in de Citrix Gateway y el acceso sin cliente.

Requisitos de tarjetas inteligentes

Usar Citrix Receiver para Windows 4.x y la aplicación Citrix Workspace 1808 para Windows o versiones posteriores 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, la compatibilidad con tarjetas inteligentes 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 Citrix Virtual Apps and Desktops, y http://www.citrix.com/ready.

Autenticarse a través de Citrix Gateway

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

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

Requisitos de Citrix Analytics Service

Puede configurar Citrix StoreFront para que la aplicación Citrix Workspace pueda enviar datos a Citrix Analytics Service. Los detalles de la configuración se describen en Citrix Analytics Service. Esta funcionalidad se admite en los casos siguientes:

- Almacenes a los que se accede desde sitios de Citrix Receiver para Web en exploradores compatibles con HTML5. Los datos de Citrix Analytics Service se proporcionan al iniciar recursos mediante la aplicación nativa de Citrix Workspace o mediante HTML5.
- Almacenes a los que se accede desde la versión 1903 de la aplicación Citrix Workspace para Windows o una versión posterior.
- Almacenes a los que se accede desde la versión 1901 de la aplicación Citrix Workspace para Linux o una versión posterior.

Planificar una implementación de StoreFront

January 6, 2020

StoreFront utiliza la tecnología Microsoft .NET que funciona en Microsoft Internet Information Services (IIS) para proporcionar los almacenes de aplicaciones de empresa que combinan recursos y ponerlos a disposición de los usuarios. StoreFront se integra con las implementaciones de Citrix Virtual Apps and Desktops para proporcionar a los usuarios un único punto de acceso de autoservicio a sus escritorios y aplicaciones.

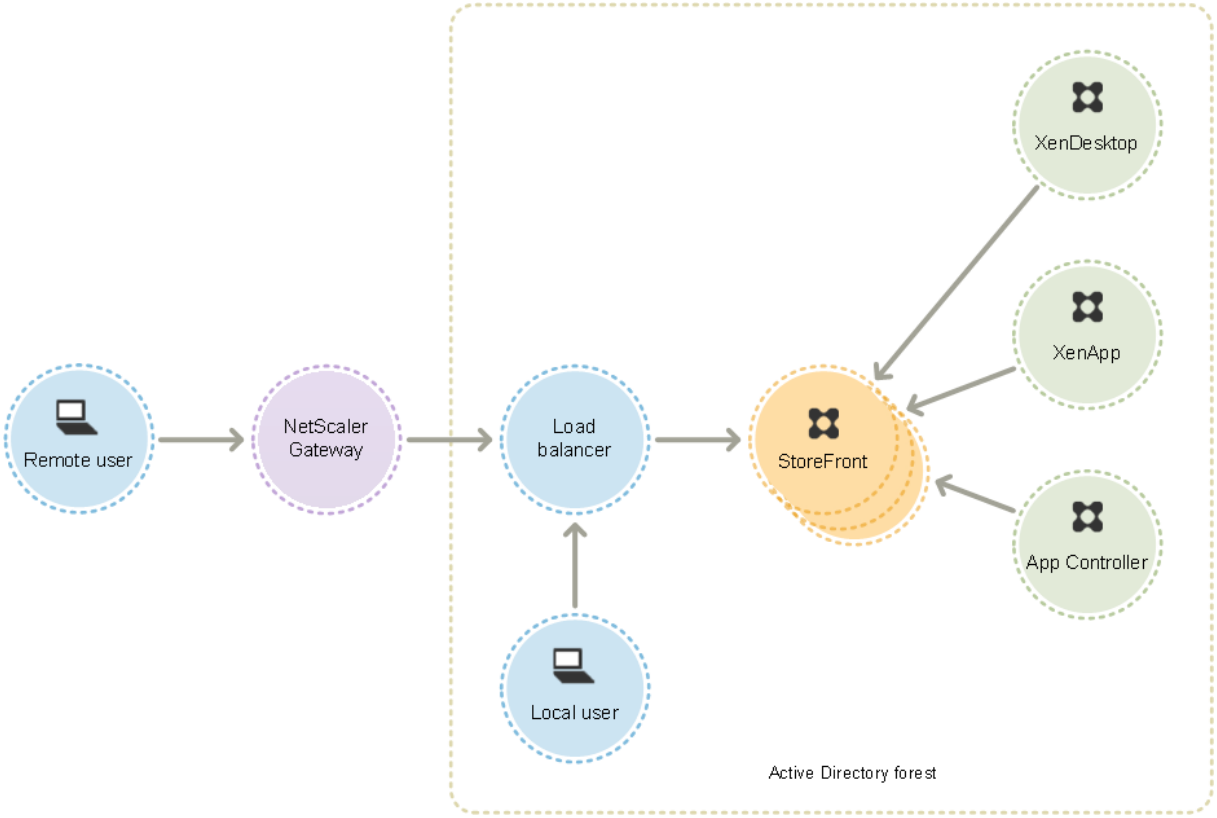
StoreFront incluye los siguientes componentes principales:

- El servicio de autenticación autentica a los usuarios para Microsoft Active Directory, lo que garantiza que dichos usuarios no necesiten iniciar sesión de nuevo para acceder a sus escritorios y aplicaciones. Para obtener más información, consulte Autenticación de usuarios.
- Los almacenes enumeran y agrupan escritorios y aplicaciones procedentes de Citrix Virtual Apps and Desktops. Los usuarios acceden a los almacenes a través de la aplicación Citrix Workspace, sitios de Citrix Receiver para Web y direcciones URL de XenApp Services. Para obtener más información, consulte Opciones de acceso de los usuarios.
- El servicio de almacenes 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 itinerantes. Para obtener más información acerca de maneras de mejorar la experiencia de los usuarios, consulte Optimizar 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 algún servidor de StoreFront deja de estar disponible por alguna razón, los usuarios pueden usar los demás servidores para seguir accediendo a sus almacenes. 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 imagen 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, Citrix ADC 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 sobre el equilibrio de carga con Citrix ADC, 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 Citrix Virtual Desktops y las comunidades de Citrix Virtual Apps 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 Citrix ADC.

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

Los valores válidos son:

- **Activado:** Este es el valor predeterminado para el nuevo 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 invertido 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).
- **Desactivado:** Este valor desactiva el bucle invertido 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
```

> **Nota:**
>
> Desactive 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 de 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 Citrix Virtual Apps and Desktops. Todos los servidores de 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 los almacenes asociados 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 piensa habilitar el acceso a StoreFront desde fuera de la red corporativa, se necesita Citrix Gateway para proteger las conexiones de los usuarios remotos. Implemente Citrix Gateway fuera de la red corporativa, con firewalls que separen Citrix Gateway de redes tanto públicas como internas. Asegúrese de que Citrix Gateway puede acceder al bosque de Active Directory que contiene los servidores de StoreFront.

Varios sitios web de Internet Information Services (IIS)

StoreFront le permite implementar distintos almacenes de aplicaciones en sitios web de IIS diferentes en cada servidor Windows, de forma que cada almacén tenga un nombre de host y un enlace de certificado diferentes.

Empiece por crear 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 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.

Ejemplo: Para crear dos implementaciones de sitio web en IIS: una para aplicaciones y otra para escritorio

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://www.storefront.app.com"
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 instalar y configurar.

Escalabilidad

La cantidad de usuarios de la aplicación Citrix Workspace que puede aceptar un único grupo de servidores de StoreFront depende del hardware que utilice y del nivel de actividad de los usuarios. En función de la actividad simulada donde los usuarios inician sesión, enumere 100 aplicaciones publicadas e inicie un recurso. Necesitará un solo servidor de StoreFront con la especificación mínima recomendada de dos CPU virtuales ejecutándose en un servidor de procesador dual Intel Xeon L5520 a 2,27 GHz subyacente para habilitar 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 de 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 la aplicación Citrix Workspace, 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:**
>
> Las implementaciones de grupos de servidores de StoreFront solo se admiten cuando los vínculos entre servidores de un grupo de servidores tienen una latencia inferior a 40 ms (con suscripciones inhabilitadas) o inferior a 3 ms (con suscripciones habilitadas). Lo ideal sería que todos los servidores de un grupo de servidores residan en la misma ubicación (centro de datos, zona de disponibilidad), pero los grupos de servidores pueden abarcar varias ubicaciones dentro de la misma región siempre que los vínculos entre los servidores del grupo cumplan estos criterios de latencia. Algunos ejemplos incluyen grupos de servidores que abarcan varias zonas de disponibilidad dentro de una región en la nube o entre centros de datos de áreas metropolitanas. Tenga en cuenta que la latencia entre zonas varía según el proveedor de la nube. Citrix no recomienda abarcar varias ubicaciones como configuración de recuperación ante desastres, pero puede ser una opción adecuada para la alta disponibilidad.
>
> No se admiten grupos de servidores de StoreFront que contengan varias versiones de sistema operativo o varios idiomas o configuraciones regionales.

Consideraciones sobre el tiempo de espera

En ocasiones, pueden darse problemas de red o de otra índole entre un almacén 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 los almacenes 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 un almacén. Establezca un valor para este parámetro de tiempo de espera que, al menos, equivalga al tiempo de espera del almacén. 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 tiempos de espera, consulte Duración del tiempo de espera de las comunicaciones y de los reintentos y Duración del tiempo de espera de las comunicaciones y de los reintentos.

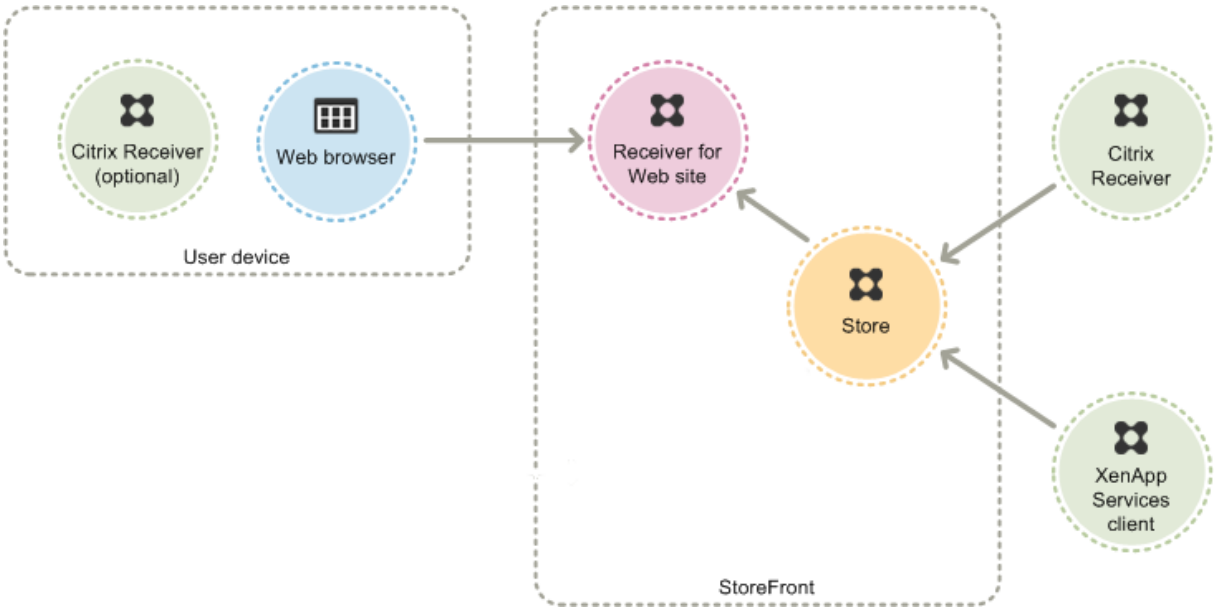
Opciones de acceso de los usuarios

January 6, 2020

Los usuarios pueden acceder a los almacenes de StoreFront mediante tres métodos distintos.

- Citrix Receiver o la aplicación Citrix Workspace: Los usuarios con versiones compatibles de Citrix Receiver o la aplicación Citrix Workspace pueden acceder a los almacenes de StoreFront desde la interfaz de usuario de Citrix Receiver o de la aplicación Citrix Workspace. Esto ofrece la mejor experiencia de usuario y la máxima funcionalidad posibles.
- Sitios de Citrix Receiver para Web: Los usuarios con exploradores web compatibles pueden acceder a los almacenes de StoreFront al dirigirse a sitios de Citrix Receiver para Web. De forma predeterminada, los usuarios también deben tener una versión compatible de Citrix Receiver o de la aplicación Citrix Workspace 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 ni la aplicación Citrix Workspace. Al crear un almacén, se crea un sitio de Citrix Receiver para Web de forma predeterminada.
- Direcciones URL de XenApp Services: Los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados con Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a los almacenes mediante la URL de XenApp Services de cada almacén. Al crear un almacén, la URL de XenApp Services correspondiente se habilita de forma predeterminada.

En la imagen se muestran las opciones de acceso a los almacenes de StoreFront:



Citrix Receiver o la aplicación Citrix Workspace

El acceso a los almacenes desde dentro de la interfaz de usuario de Citrix Receiver o de la aplicación Citrix Workspace ofrece la mejor experiencia de usuario y la mayor funcionalidad posibles. Para ver las versiones de Citrix Receiver o de la aplicación Citrix Workspace que pueden usarse para acceder a los almacenes de esta manera, consulte Requisitos del sistema. Las menciones de "aplicación Citrix Workspace" de este documento también representan las versiones compatibles de Citrix Receiver, a menos que se indique lo contrario.

La aplicación Citrix Workspace utiliza direcciones URL internas y externas como balizas. Al intentar ponerse en contacto con estas balizas, la aplicación Citrix Workspace puede determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un escritorio o a una aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan devolver los correspondientes datos de conexión a la aplicación Citrix Workspace. Esto permite que la aplicación Citrix Workspace se asegure de no pedir a los usuarios que vuelvan a iniciar sesión al acceder a un escritorio o a una aplicación. Para obtener más información, consulte Configurar balizas.

Después de la instalación, la aplicación Citrix Workspace debe configurarse con los datos de conexión de los almacenes 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, la aplicación Citrix Workspace requiere conexiones HTTPS a los almacenes. 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 Configurar e instalar mediante parámetros de línea de comandos en la documentación de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows.

Archivos de aprovisionamiento

Es posible proporcionar a los usuarios archivos de aprovisionamiento que contengan los datos de conexión a sus almacenes. Después de instalar la aplicación Citrix Workspace, los usuarios pueden abrir el archivo .cr para configurar automáticamente las cuentas para los almacenes. De forma predeterminada, los sitios de Citrix Receiver para Web ofrecen a los usuarios un archivo de aprovisionamiento para el único almacén para el que esté configurado el sitio en cuestión. Puede indicar a los usuarios que visiten los sitios de Receiver para Web de los almacenes a los que deseen tener acceso y descarguen los archivos de aprovisionamiento desde esos sitios. También, para lograr un mayor

control, puede usar la consola de administración de Citrix StoreFront para generar archivos de aprovisionamiento que contengan los datos de conexión para uno o más almacenes. A continuación, puede distribuir estos archivos a los usuarios adecuados. Para obtener más información, consulte Exportar archivos de aprovisionamiento de almacenes para los usuarios.

Direcciones URL de configuración generadas automáticamente

Para los usuarios con macOS, es posible utilizar Setup URL Generator de Citrix Receiver para Mac o la aplicación Citrix Workspace para Mac con el fin de crear una URL que contenga los datos de conexión de un almacén. Después de instalar la aplicación Citrix Workspace, los usuarios pueden hacer clic en la URL para configurar automáticamente una cuenta para el almacén. 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 introducir direcciones URL de almacén en la aplicación Citrix Workspace para crear cuentas. Para obtener más información, consulte la documentación de la aplicación Citrix Workspace.

Detección de cuentas basada en direcciones de correo electrónico

Los usuarios que instalen por primera vez la aplicación Citrix Workspace en un dispositivo pueden configurar cuentas con sus direcciones de correo electrónico si descargan la aplicación Citrix Workspace del sitio web de Citrix o de una página de descarga de la aplicación Citrix Workspace alojada en la red interna. Puede configurar los registros SRV de los recursos del localizador de Citrix Gateway o StoreFront en su servidor DNS de Active Directory de Microsoft. Los usuarios no necesitan conocer la información de acceso a los almacenes; simplemente deben introducir sus direcciones de correo electrónico durante la configuración inicial de la aplicación Citrix Workspace. La aplicación Citrix Workspace 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 los almacenes a los que los usuarios pueden acceder mediante la aplicación Citrix Workspace.

Configurar 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 la aplicación Citrix Workspace por primera vez en un dispositivo puedan configurar sus cuentas con sus direcciones de correo electrónico. Siempre que descarguen la aplicación Citrix Workspace desde el sitio web de Citrix o una página de descarga de la aplicación Citrix Workspace

alojada en su red interna, los usuarios no necesitan conocer los detalles de acceso de sus almacenes cuando instalan y configuran la aplicación Citrix Workspace. La detección de cuentas basada en direcciones de correo electrónico está disponible si la aplicación Citrix Workspace se descarga desde cualquier otra ubicación, como desde un sitio de Receiver para Web. Tenga en cuenta que los archivos *ReceiverWeb.exe* o *ReceiverWeb.dmg* descargados desde Citrix Receiver para Web no piden a los usuarios que configuren un almacén. Los usuarios aún pueden utilizar la opción Agregar cuenta e introducir su correo electrónico.

Durante el proceso de configuración inicial, la aplicación Citrix Workspace pide a los usuarios que introduzcan una dirección de correo electrónico o una URL de almacén. Cuando un usuario introduce una dirección de correo electrónico, la aplicación Citrix Workspace 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 almacenes disponibles en la que el usuario pueda seleccionarlos.

Para permitir que la aplicación Citrix Workspace busque los almacenes disponibles en función de las direcciones de correo electrónico de los usuarios, configure los registros SRV de los recursos del localizador para Citrix Gateway o StoreFront en el servidor DNS. Como alternativa, también puede implementar StoreFront en un servidor denominado “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, la aplicación Citrix Workspace busca una máquina denominada “discoverReceiver” para identificar un servidor de StoreFront.

Para permitir la detección de cuentas basada en direcciones de correo electrónico, es necesario instalar un certificado de servidor válido en el dispositivo Citrix Gateway o en el servidor de 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 del tipo Sujeto o Nombre alternativo del sujeto de discoverReceiver.dominio, donde “dominio” 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 la aplicación Citrix Workspace se conecte por primera vez al servidor de StoreFront. La detección de cuentas basada en correo electrónico no se puede usar con ninguna otra identidad de certificado.[](/en-us/netscaler-gateway/12-1/storefront-integration/ng-clg-session-policies-overview-con/ng-clg-storefront-policies-con/ng-clg-storefront-email-discovery-tsk.html)

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 Citrix Gateway con los datos de conexión de StoreFront. Para obtener más información, consulte Conectarse a StoreFront mediante la detección basada en direcciones de correo electrónico.

Agregar un registro SRV a un servidor DNS

1. En la pantalla de **Inicio** de Windows, haga clic en **Herramientas administrativas** y, a continuación, haga clic en **DNS** (sistema de normas de dominio) en la carpeta **Herramientas administrativas**.
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 Citrix Gateway (para admitir a usuarios locales y remotos) o el servidor de StoreFront (para admitir solamente a los usuarios de la red local) con el formato nombre de *servidor.dominio:puerto*.

   Si su entorno incluye servidores DNS internos y externos, puede agregar un registro SRV que especifique el FQDN del servidor de StoreFront en su servidor DNS interno y otro registro en su servidor externo que especifique el FQDN de Citrix Gateway. 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 Citrix Gateway.
7. Si ha configurado un registro SRV para el dispositivo Citrix Gateway, agregue los datos de conexión de StoreFront a Citrix 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 los almacenes de StoreFront al navegar a sitios de Citrix Receiver para Web. Al crear un almacén, se crea automáticamente un sitio de Citrix Receiver para Web vinculado a él. La configuración predeterminada de los sitios de Citrix Receiver para Web requiere que los usuarios instalen una versión compatible de la aplicación Citrix Workspace para acceder a sus escritorios y aplicaciones. Para obtener más información acerca de las combinaciones de la aplicación Citrix Workspace y exploradores 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 la aplicación Citrix Workspace está instalada en el dispositivo de usuario. Si no se detecta la aplicación Citrix Workspace, se solicita al usuario que la descargue y la instale para 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 de StoreFront y proporcionar a los usuarios estos archivos locales. El almacenamiento local de los archivos de instalación de la aplicación Citrix Workspace 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 sobre cómo configurar la implementación de Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows y Citrix Receiver para Mac o la aplicación Citrix Workspace para Mac, consulte Configurar sitios de Citrix Receiver para web.

Aplicación Citrix Workspace para HTML5

La aplicación Citrix Workspace para HTML5 es un componente de StoreFront que está integrado de manera predeterminada en los sitios de Citrix Receiver para Web. Puede habilitar la aplicación Citrix Workspace para HTML5 en los sitios de Citrix Receiver para Web. De este modo, los usuarios tendrán acceso a sus recursos aunque no puedan instalar la aplicación Citrix Workspace. Con la aplicación Citrix Workspace para HTML5, los usuarios pueden acceder a escritorios y aplicaciones directamente desde exploradores web compatibles con HTML5 sin necesidad de instalar la aplicación Citrix Workspace. Cuando se crea un sitio, la aplicación Citrix Workspace para HTML5 está inhabilitada de forma predeterminada. Para obtener más información sobre cómo habilitar la aplicación Citrix Workspace para HTML5, consulte citrix-receiver-download-page-template.html.

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

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

De manera predeterminada, el acceso a través de la aplicación Citrix Workspace para HTML5 para los recursos proporcionados por Citrix Virtual Apps and Desktops se encuentra inhabilitado para los usuarios locales de la red interna. Para habilitar el acceso local a escritorios y aplicaciones mediante la aplicación Citrix Workspace para HTML5, debe habilitar la directiva Conexiones de WebSockets en los servidores Citrix Virtual Apps and Desktops. Asegúrese de que los firewalls y otros dispositivos

de red permiten el acceso al puerto de la aplicación Citrix Workspace para HTML5 especificado en la directiva. Para obtener más información, consulte Configuraciones de directiva de WebSockets.

De forma predeterminada, la aplicación Citrix Workspace para HTML5 inicia los escritorios y las aplicaciones en una ficha nueva del explorador. No obstante, cuando los usuarios inician recursos con la aplicación Citrix Workspace para HTML5 a partir de accesos directos, el escritorio o la aplicación reemplazan el sitio de Citrix Receiver para Web en la ficha existente del explorador en vez de aparecer en una nueva ficha. Puede configurar la aplicación Citrix Workspace para HTML5 para que los recursos se inicien siempre en la ficha del sitio de Receiver para Web. Para obtener más información, consulte Configurar el uso de fichas del explorador web con la aplicación Citrix Workspace 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 Configurar 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 la aplicación Citrix Workspace o deben usar la aplicación Citrix Workspace para HTML5 si quieren 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 la aplicación Citrix Workspace 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 quiere 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 Citrix 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 Citrix Gateway para limitar el acceso de los usuarios a solamente esos sitios específicos. Para obtener más información, consulte http://support.citrix.com/article/CTX123610.

Personalizar 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 los almacenes a través de un sitio de Citrix Receiver para Web se benefician de muchas de las funciones disponibles mediante el acceso a almacenes con la aplicación Citrix Workspace, 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 los almacenes, tenga en cuenta las siguientes restricciones.

- A través de un sitio de Citrix Receiver para Web solo se puede acceder a un único almacén.
- 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 Citrix 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 un almacén 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 los almacenes. 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.

- La aplicación Citrix Workspace 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 mediante Citrix Gateway.
- Para utilizar la aplicación Citrix Workspace 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.

Direcciones URL de XenApp Services

Los usuarios con versiones anteriores de clientes Citrix que no se pueden actualizar pueden acceder a los almacenes mediante la configuración de sus clientes con la URL de XenApp Services para un almacén. También puede habilitar el acceso a los almacenes a través de las direcciones URL de XenApp Services desde dispositivos de escritorio unidos a un dominio y equipos reasignados que tengan 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 de StoreFront.

StoreFront admite la autenticación PassThrough con tarjetas de proximidad a través de la aplicación Citrix Workspace para las direcciones URL de XenApp Services. En los productos asociados de Citrix Ready, se utiliza Citrix Fast Connect API para optimizar los inicios de sesión a través de Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows y conectarse a los almacenes con la URL de XenApp Services. Los usuarios se autentican en estaciones de trabajo mediante tarjetas de proximidad y se conectan rápidamente a los escritorios y las aplicaciones que proporcionan Citrix Virtual Apps and Desktops. Para obtener más información, consulte la documentación más reciente de Citrix Receiver para Windows.

Al crear un almacén, la URL de XenApp Services correspondiente se habilita de forma predeterminada. La URL de XenApp Services de un almacén tiene el formato http[s]://serveraddress/Citrix/storename/PNAgent/conf donde serveraddress es el nombre de dominio completo del servidor o del entorno con carga equilibrada de la implementación de StoreFront, mientras que storename es el nombre especificado para el almacén cuando se creó. Esto permite que las aplicaciones Citrix Workspace que solo pueden usar el protocolo PNAgent puedan conectarse a StoreFront. Para saber los clientes que pueden utilizarse para acceder a almacenes mediante las direcciones URL de XenApp Services, consulte Requisitos del dispositivo del usuario.

Consideraciones importantes

Las direcciones URL de XenApp Services se han diseñado para los usuarios que no pueden actualizar su versión a la de la aplicación Citrix Workspace y para los casos en que no están disponibles otros

métodos de acceso. A la hora de optar por utilizar las direcciones URL de XenApp Services para proporcionar a los usuarios acceso a los almacenes, tenga en cuenta las siguientes restricciones.

- No se puede modificar la URL de XenApp Services para un almacén.
- No se puede modificar la configuración de la URL de XenApp Services mediante la edición del archivo de configuración, config.xml.
- Las direcciones URL de XenApp Services admiten 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 XenApp Services, y solo está disponible una dirección URL por almacén. Para habilitar varios métodos de autenticación, debe crear almacenes independientes, cada uno con una URL de XenApp Services, para cada método de autenticación. Los usuarios deben conectarse al almacén adecuado 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 XenApp Services y no se puede configurar ni inhabilitar.
- Las solicitudes de los usuarios para cambiar sus contraseñas se dirigen al controlador de dominio directamente a través de servidores Citrix Virtual Apps and Desktops que proporcionan escritorios y aplicaciones para el almacén. De esta forma, se omite el servicio de autenticación de StoreFront.

Autenticación de usuarios

March 2, 2020

StoreFront admite diversos métodos de autenticación para los usuarios que acceden a los almacenes, 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 se inhabilitan de forma predeterminada cuando se crea el primer almacén. 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 los almacenes. 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 Citrix Gateway para acceder a Citrix Receiver para Web, Citrix Gateway se ocupa del inicio de sesión y del cambio de contraseña cuando esta 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 Citrix Gateway termina y el usuario tiene que volver a iniciar la sesión. Los usuarios de Citrix Receiver para Linux o de la aplicación Citrix Workspace 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 almacenes. StoreFront puede admitir la autenticación SAML directamente dentro de la red corporativa, sin tener que ir a través de Citrix Gateway.

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 (IdP) compatibles con SAML 2.0:
  - Microsoft AD FS 4.0 (Windows Server 2016) solo con enlaces SAML (enlaces que no sean de WS-Federation). Para obtener más información, consulte Implementación de los Servicios de federación de Microsoft Active Directory 2016 y Operaciones de los Servicios de federación de Microsoft Active Directory 2016.
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - Citrix Gateway (configurado como proveedor de identidades)
- Puede configurar la autenticación SAML en StoreFront desde la consola de administración de StoreFront en una nueva implementación (consulte Crear una implementación) o en una implementación existente (consulte Configurar el servicio de autenticación). También puede configurar la autenticación de SAML mediante cmdlets de PowerShell, consulte SDK de StoreFront.
- Citrix Receiver (4.6 o una versión posterior) o la aplicación Citrix Workspace para Windows, o bien Citrix Receiver para Web.

El uso de la autenticación SAML en Citrix Gateway se admite actualmente en sitios de Receiver para Web.

PassThrough de dominio

Los usuarios realizan la autenticación en equipos Windows que pertenecen a un dominio, y sus credenciales se usan para iniciar sesión automáticamente cuando acceden a los almacenes.

Al instalar StoreFront, la autenticación PassThrough de dominio está inhabilitada de forma predeterminada. La autenticación PassThrough de dominio puede habilitarse para los usuarios que se conectan a almacenes a través de la aplicación Citrix Workspace y direcciones URL de XenApp Services. Los sitios de Citrix Receiver para Web admiten la autenticación PassThrough de dominio para Internet Explorer, Microsoft Edge, Mozilla Firefox y Google Chrome en máquinas cliente de Windows.

Para habilitar la autenticación PassThrough de dominio

1. Instale Citrix Receiver para Windows, la aplicación Citrix Workspace para Windows o el plug-in de Citrix Online para Windows en los dispositivos de usuario. Compruebe que la autenticación PassThrough está habilitada.
2. Habilite la autenticación PassThrough de dominio en el nodo del sitio de Receiver para Web que hay en la consola de administración.
3. Configure SSON en Citrix Receiver para Windows o en la aplicación Citrix Workspace para Windows; procedimiento descrito en Configurar la autenticación PassThrough de dominio. La aplicación Citrix Workspace para HTML5 no admite la autenticación PassThrough de dominio.
4. El comportamiento predeterminado de Windows es el "inicio de sesión automático solo en la zona de la intranet". Para Internet Explorer, Mozilla Firefox y Google Chrome, configure los sitios de Citrix Receiver para Web como sitios de la intranet desde "Opciones de Internet" o habilite el inicio de sesión automático para la zona de confianza. Para Microsoft Edge, debe configurar los sitios de Citrix Receiver para Web como sitios de la intranet.
5. Para Mozilla Firefox, modifique la configuración avanzada del explorador para que confíe en el URI de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows.

   > Advertencia:
   >
   > Modificar incorrectamente la configuración avanzada puede causar problemas graves. Por tanto, las modificaciones serán bajo su propia responsabilidad.

   a) Inicie Firefox, escriba **about:config** en el campo de dirección y seleccione "¡Acepto el riesgo!".
   b) Escriba **ntlm** en el cuadro de búsqueda.
   c) Haga doble clic en "network.automatic-ntlm-auth.trusted-uris" y escriba la URL del sitio de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows en el cuadro de diálogo emergente.
   d) Haga clic en **Aceptar**.

PassThrough desde Citrix Gateway

Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes. La autenticación PassThrough desde Citrix Gateway está habilitada de forma predeterminada al configurar el acceso remoto a un almacén. Los usuarios pueden conectarse a través de Citrix Gateway a los almacenes mediante sitios de Citrix Receiver o la aplicación Citrix Workspace. Para obtener más información sobre cómo configurar el acceso a StoreFront a través de Citrix Gateway, consulte Agregar una conexión de Citrix Gateway.

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

- **Token de seguridad.** Los usuarios inician sesión en Citrix Gateway mediante códigos de acceso derivados de tokencodes generados por tokens de seguridad combinados, en algunos casos, con códigos 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 Citrix Gateway deben introducir sus credenciales de dominio y los códigos de acceso de tokens de seguridad.
- **Certificado del cliente.** Los usuarios inician sesión en Citrix Gateway y su autenticación se produce basándose en los atributos del certificado del cliente que se presenta ante Citrix Gateway. Configure la autenticación de certificados del cliente para permitir que los usuarios inicien sesión en Citrix Gateway mediante 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 Citrix 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 Citrix Gateway con una contraseña. Para configurar la autenticación PassThrough desde Citrix Gateway para el acceso a StoreFront por parte de usuarios de tarjeta inteligente, delegue la validación de credenciales en Citrix Gateway. Para obtener más información, consulte Creación y configuración del servicio de autenticación.

Los usuarios pueden conectarse a almacenes en la aplicación Citrix Workspace con la autenticación PassThrough a través del túnel VPN SSL mediante el plug-in de Citrix Gateway. Los usuarios remotos que no pueden instalar el plug-in de Citrix Gateway pueden utilizar el acceso sin cliente para conectarse a los almacenes en la aplicación Citrix Workspace con la autenticación PassThrough. Para utilizar el acceso sin cliente con el fin de conectarse a los almacenes, los usuarios necesitan una versión de la aplicación Citrix Workspace 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 ello, configure Citrix Gateway de modo que funcione como proxy remoto

seguro. Los usuarios inician sesión directamente en Citrix 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 el plug-in de Citrix Gateway.

Si quiere configurar la autenticación de doble origen en Citrix Gateway para usuarios remotos que accedan a los almacenes desde la aplicación Citrix Workspace, debe crear dos directivas de autenticación en Citrix 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. Cuando agregue el dispositivo Citrix Gateway a su configuración de StoreFront, configure 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 multidominio a través de Citrix Gateway en StoreFront, configure el atributo de nombre del SSO en userPrincipalName en la directiva de autenticación LDAP de Citrix Gateway para cada dominio. Es posible que deba especificar un dominio a los usuarios en la página de inicio de sesión de Citrix Gateway para que se pueda determinar la directiva de LDAP correspondiente. Al configurar los perfiles de sesión de Citrix 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 Citrix Gateway lo admita, puede utilizar SmartAccess para controlar el acceso de los usuarios a los recursos de Citrix Virtual Apps and Desktops en función de las directivas de sesión de Citrix Gateway. Para obtener más información sobre SmartAccess, consulte Cómo funciona SmartAccess para Citrix Virtual Apps and Desktops.

Tarjetas inteligentes

Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a los almacenes. 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 los almacenes a través de la aplicación Citrix Workspace, Citrix Receiver para Web y las direcciones URL de XenApp Services.

Use la autenticación con tarjeta inteligente para agilizar el proceso de inicio de sesión para sus usuarios y al mismo tiempo mejorar la seguridad del acceso de los usuarios a su 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 Citrix Virtual Apps and Desktops. 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.

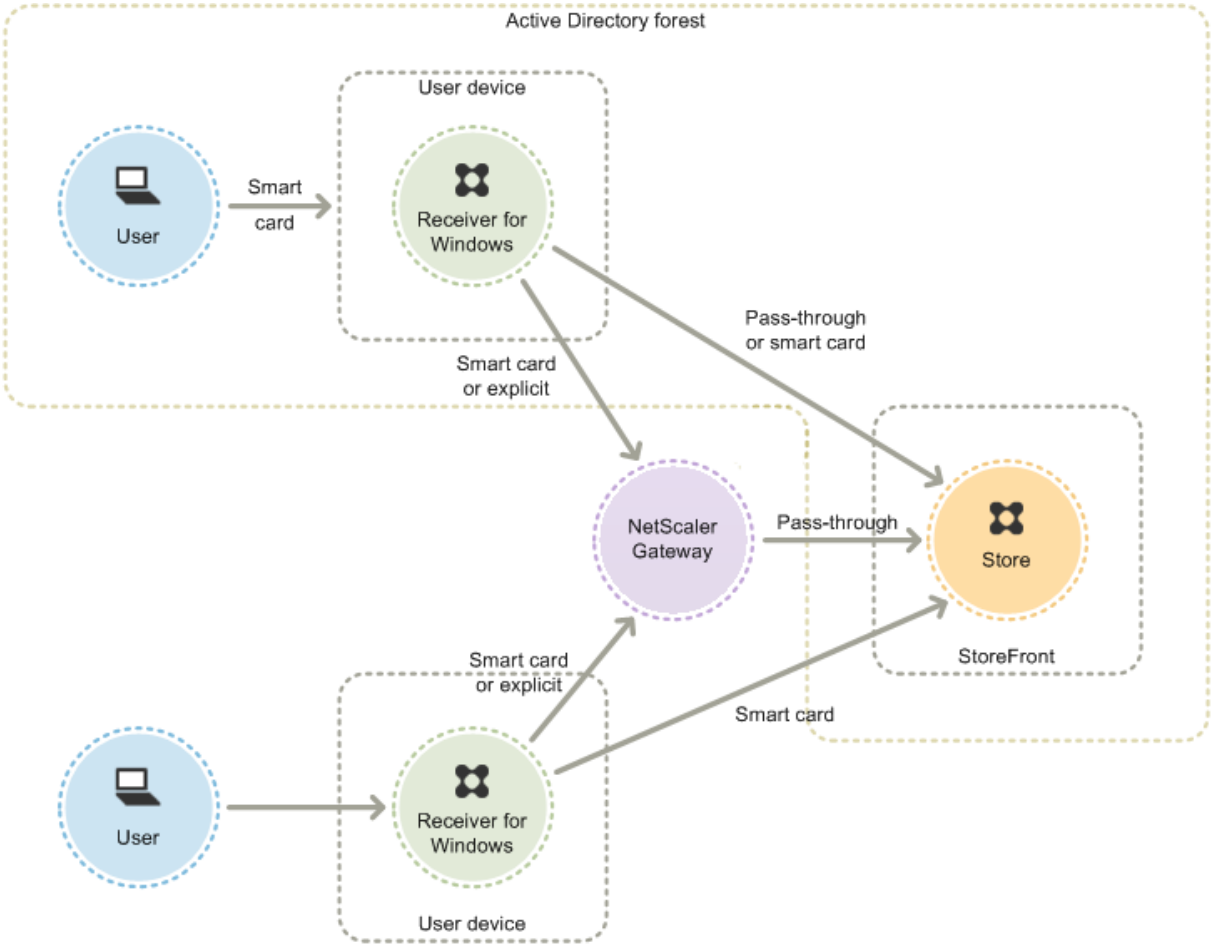
Para habilitar la autenticación con tarjeta inteligente, las cuentas de los usuarios deben configurarse ya sea en el dominio de Microsoft Active Directory que contiene los servidores de StoreFront, o bien, en un dominio que tenga una relación de confianza bidireccional directa con el dominio del servidor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

Usar tarjetas inteligentes con Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows

Los usuarios con dispositivos con Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows se pueden autenticar con tarjetas inteligentes, ya sea directamente o a través de Citrix 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 o de la aplicación Citrix Workspace 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 con 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 o la aplicación Citrix Workspace 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 o la aplicación Citrix Workspace 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 o la aplicación Citrix Workspace 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 Citrix Gateway deben iniciar la sesión mediante 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 mediante 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 Citrix Gateway en StoreFront y delegar la validación de credenciales en Citrix Gateway. Después, cree un servidor virtual adicional de Citrix Gateway a través del cual se redirigirán las conexiones de usuario hacia sus recursos. En el caso de dispositivos unidos a un dominio, también debe configurar Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows para la autenticación PassThrough.

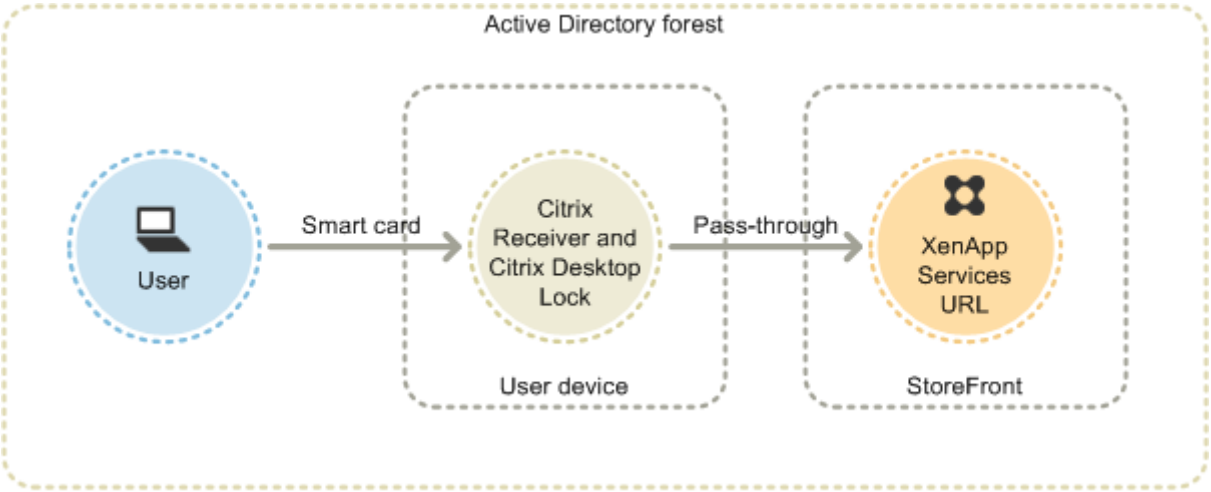
> **Nota:**
>
> Si utiliza Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows, puede configurar un segundo servidor virtual y usar la puerta de enlace óptima para eliminar la necesidad de solicitar el PIN al iniciar aplicaciones y escritorios.

Los usuarios pueden iniciar sesión en Citrix 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 Citrix Gateway. Configure la autenticación PassThrough desde Citrix Gateway a StoreFront y delegue la validación de las credenciales a Citrix Gateway para los usuarios de tarjeta inteligente, de modo que los usuarios se autentiquen silenciosamente en StoreFront.

Uso de tarjetas inteligentes con las direcciones URL de XenApp Services

Los usuarios 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 XenApp Services.

La imagen muestra la autenticación con tarjeta inteligente desde un dispositivo de escritorio (Desktop Appliance) unido a un dominio que se ejecuta en 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 XenApp Services. Los usuarios se autentican automáticamente cuando acceden a sus escritorios y a sus aplicaciones, y no tienen que volver a introducir su PIN.

Usar tarjetas inteligentes en Citrix Receiver para Web

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

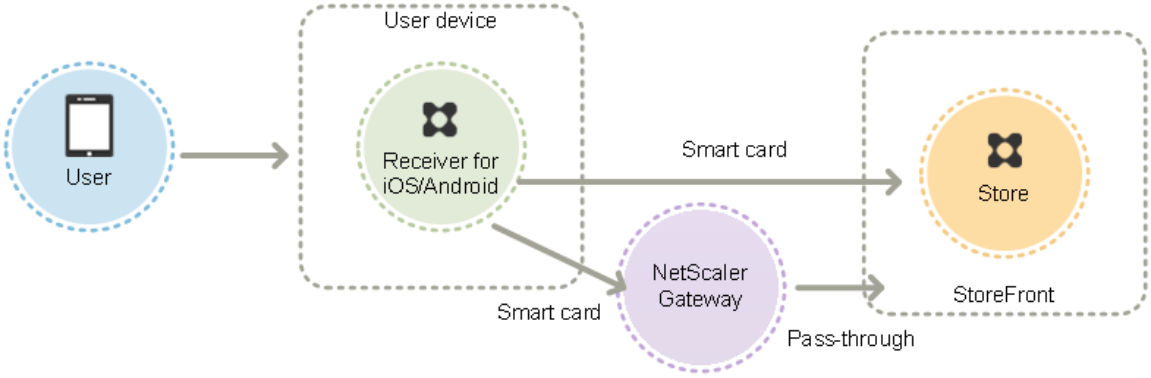
1. Seleccione el nodo Citrix Receiver para Web del panel de la izquierda.
2. Seleccione el sitio en el que quiere usar la autenticación con tarjeta inteligente.
3. Seleccione la tarea Elegir métodos de autenticación del panel de la derecha.
4. Marque la casilla Tarjeta inteligente en la pantalla de diálogo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

Si habilita la autenticación PassThrough con tarjeta inteligente en Citrix Virtual Apps and Desktops para los usuarios de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows con dispositivos unidos a un dominio que no acceden a los almacenes a través de Citrix Gateway, este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear almacenes independientes para cada método de autenticación. Los usuarios deben conectarse al almacén adecuado para su método de autenticación.

Si habilita la autenticación PassThrough con tarjeta inteligente en Citrix Virtual Apps and Desktops para los usuarios de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows con dispositivos unidos a un dominio que acceden a los almacenes a través de Citrix Gateway, este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar la autenticación PassThrough para algunos usuarios y solicitar a otros usuarios que inicien sesión en los escritorios y aplicaciones, debe crear almacenes independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.

Usar tarjetas inteligentes en la aplicación Citrix Workspace para iOS y Android

Los usuarios con dispositivos con la aplicación Citrix Workspace para Windows para iOS o Android se pueden autenticar con tarjetas inteligentes, ya sea directamente o a través de Citrix 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 el almacén 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 estas aplicaciones Citrix Workspace, tiene la opción de especificar tarjetas inteligentes o credenciales de dominio. Si ha creado un almacén para usar tarjetas inteligentes y quiere conectarse al mismo almacén mediante credenciales de dominio, debe agregar un almacén independiente sin activar las tarjetas inteligentes.

Los usuarios que se conectan a través de Citrix Gateway deben iniciar la sesión mediante su tarjeta inteligente y su PIN al menos dos veces para acceder a sus escritorios y aplicaciones. Los usuarios se autentican mediante 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 Citrix Gateway en StoreFront y delegar la validación de credenciales en Citrix Gateway. Después, cree un servidor virtual adicional de Citrix Gateway a través del cual se redirigirán las conexiones de usuario hacia sus recursos.

Los usuarios pueden iniciar sesión en Citrix 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 desde Citrix Gateway a StoreFront y delegue la validación de las credenciales a Citrix 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.

Usar tarjetas inteligentes con Citrix Receiver para Linux o la aplicación Citrix Workspace para Linux

Los usuarios con dispositivos con Citrix Receiver para Linux o la aplicación Citrix Workspace 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, ni Citrix Receiver para Linux ni la aplicación Citrix Workspace para Linux tienen mecanismo alguno 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 o la aplicación Citrix Workspace para Windows. Consulte Configurar la autenticación con tarjeta inteligente y, para obtener instrucciones sobre el 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 o en la aplicación Citrix Workspace 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 directamente en Citrix Receiver para Linux o en la aplicación Citrix Workspace para Linux, 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 Citrix Gateway deben iniciar la sesión mediante su tarjeta inteligente y su PIN al menos una vez para acceder a sus escritorios y 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 Citrix Gateway en StoreFront y delegar la validación de credenciales en Citrix Gateway. Después, cree un servidor virtual adicional de Citrix Gateway a través del cual se redirigirán las conexiones de usuario hacia sus recursos.

Los usuarios pueden iniciar sesión en Citrix 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 Citrix Gateway. Configure la autenticación PassThrough desde Citrix Gateway a StoreFront y delegue la validación de las credenciales a Citrix 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 o para la aplicación Citrix Workspace para Linux no se admiten en los sitios de asistencia de XenApp Services.

Una vez que la compatibilidad con tarjetas inteligentes se haya habilitado tanto para el servidor como

para la aplicación Citrix Workspace, y siempre que la directiva de aplicación de los certificados de tarjeta inteligente lo permita, puede utilizar tarjetas inteligentes con los siguientes fines:

- Autenticación de inicio de sesión con tarjetas inteligentes. Utilice tarjetas inteligentes para autenticar usuarios en servidores Citrix Virtual Apps and Desktops.
- Soporte para aplicaciones de tarjetas inteligentes. Habilite las aplicaciones publicadas compatibles con tarjetas inteligentes para que puedan acceder a dispositivos de tarjetas inteligentes locales.

Usar tarjetas inteligentes en XenApp Services

Los usuarios que inician sesión en los sitios de soporte de XenApp Services para iniciar aplicaciones y escritorios se pueden autenticar mediante tarjetas inteligentes sin depender de ningún hardware, sistema operativo o aplicación Citrix Workspace específicos. Cuando un usuario accede a un sitio de soporte de XenApp Services 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 método de autenticación con tarjeta inteligente en XenApp Services, consulte Configuración de la autenticación de las direcciones URL de XenApp Services.

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 el plug-in de Citrix Gateway, iniciar sesión a través de una página web y utilizar las tarjetas inteligentes y los PIN en cada paso de la autenticación. La autenticación PassThrough

en StoreFront con el plug-in de Citrix Gateway 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 quiere 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 Citrix Virtual Apps and Desktops para los usuarios de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows con dispositivos unidos a un dominio que no acceden a los almacenes a través de Citrix Gateway, este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear almacenes independientes para cada método de autenticación. Los usuarios deben conectarse al almacén adecuado para su método de autenticación.
- Si habilita la autenticación PassThrough con tarjeta inteligente en Citrix Virtual Apps and Desktops para los usuarios de Citrix Receiver para Windows o de la aplicación Citrix Workspace para Windows con dispositivos unidos a un dominio que acceden a los almacenes a través de Citrix Gateway, este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar la autenticación PassThrough para algunos usuarios y solicitar a otros usuarios que inicien sesión en los escritorios y aplicaciones, debe crear almacenes independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.
- Solo se puede configurar un método de autenticación para cada dirección URL de XenApp Services, y solo está disponible una dirección URL por almacén. Si quiere habilitar otros tipos de autenticación (además de la autenticación con tarjeta inteligente), debe crear almacenes independientes, cada uno de ellos con una URL de XenApp Services, para cada método de autenticación. A continuación, debe dirigir a los usuarios al almacén adecuado 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 los almacenes deben colocarse en el mismo servidor. Debe usar un certificado del cliente válido para todos los almacenes. Con esta configuración de sitio de IIS, los usuarios de tarjetas inteligentes no pueden conectarse a través de Citrix Gateway y no pueden utilizar la autenticación explícita. Los usuarios deben iniciar sesión de nuevo si quitan las tarjetas inteligentes de los dispositivos.

Optimizar la experiencia de usuario

January 6, 2020

StoreFront incluye funciones diseñadas para mejorar la experiencia de usuario. Estas funciones se configuran de forma predeterminada cuando se crean almacenes y los correspondientes sitios de Citrix Receiver para Web y direcciones URL de XenApp Services 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 los almacenes a través de las direcciones URL de XenApp Services. 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 un almacén, ya sea mediante el sitio de Citrix Receiver para Web o la URL de XenApp Services, e inicia algunas aplicaciones. Si, a continuación, el usuario inicia sesión en el mismo almacén, 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 un almacén específica se desconectan automáticamente (pero no se cierran) cuando el usuario cierra sesión en el almacén. 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 XenApp Services 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 Configurar el 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 la aplicación Citrix Workspace se encuentra instalada en los dispositivos de los usuarios, o bien si se utiliza la aplicación Citrix Workspace 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 área 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 la aplicación Citrix Workspace 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 Citrix Virtual Apps and Desktops. La asociación de tipos de archivos está habilitada de forma predeterminada en los almacenes nuevos. Para obtener más información, consulte Inhabilitar la asociación de tipos de archivo.

Cambio de contraseña por parte de los usuarios

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.

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 cambiar las contraseñas, algunas funciones importantes de seguridad se dejan a merced de cualquier persona que pueda acceder a los almacenes a través del 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 los almacenes 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. Lo primero que ven los usuarios es el escritorio al iniciar sesión en el sitio. Independientemente de que también sea posible acceder a las aplicaciones desde el sitio de Citrix Receiver para Web, si existe un solo escritorio disponible para un usuario, Receiver para Web inicia automáticamente ese escritorio cuando el usuario inicia 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 Configurar cómo 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 Citrix Virtual Desktops 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 los almacenes a través de la aplicación Citrix Workspace o las direcciones URL de XenApp Services, el cliente Citrix determina la manera en que se muestran los escritorios, las aplicaciones y su comportamiento.

Recomendaciones adicionales

Cuando entregue aplicaciones con Citrix Virtual Apps and Desktops, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a las aplicaciones a través de los almacenes: Para obtener más información acerca de la entrega de aplicaciones, consulte Creación de una aplicación para un 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 creadas en Citrix Virtual Apps and Desktops aparecen como categorías de la aplicación Citrix Workspace. Podría, por ejemplo, agrupar aplicaciones según el tipo o, si no, crear carpetas para diferentes roles de usuario en su organización.
- Asegúrese de poner descripciones pertinentes cuando entrega las aplicaciones, dado que estas descripciones serán visibles para los usuarios de la aplicación Citrix Workspace.
- Puede especificar que todos los usuarios tengan un conjunto básico de aplicaciones "obligatorias" que no se pueden quitar de la página de inicio de la aplicación Citrix Workspace. 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 un almacén 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 el almacén, 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 un almacén a una aplicación web o de software como servicio (SaaS) administrada por App Controller, marque la casilla **App is available in Citrix Receiver or Citrix Workspace app to all users automatically** (Aplicación automáticamente disponible en Citrix Receiver o en la aplicación Citrix Workspace para todos los usuarios) al configurar los parámetros de la aplicación.
- Para anunciar aplicaciones de Citrix Virtual Apps and Desktops a los usuarios o facilitar la búsqueda de las aplicaciones más utilizadas, incorpórelas a la lista Destacados de la aplicación Citrix Workspace. Para ello, agregue la cadena `KEYWORDS:Featured` a la descripción de las aplicaciones.

> **Nota:**
>
> 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 Citrix Virtual Apps and Desktops 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, *aplicación* 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, la aplicación Citrix Workspace busca el nombre especificado o la ruta de acceso en el dispositivo de usuario para determinar si la aplicación ya está instalada localmente. Si se encuentra la aplicación, la aplicación Citrix Workspace suscribe al usuario a la aplicación entregada, pero no crea un acceso directo. Cuando el usuario inicia la aplicación entregada desde la aplicación Citrix Workspace, se ejecuta la instancia instalada localmente. Para obtener más información, consulte Configurar la entrega de aplicaciones.
- En Citrix Virtual Apps and Desktops, cuando los usuarios inician una aplicación publicada desde un escritorio publicado, puede controlar si la aplicación se inicia en esa sesión de escritorio o como una aplicación publicada en el mismo grupo de entrega. Use un cmdlet de PowerShell en el Broker Service y una configuración de directiva en Citrix Receiver para Windows (vPrefer) para controlar este comportamiento. Esta función solo funciona con el inicio de aplicaciones publicadas con Citrix Receiver para Windows o con la aplicación Citrix Workspace para Windows. No se puede utilizar para iniciar una aplicación localmente si la aplicación publicada se lanza a través del sitio de StoreFront en un explorador web. En versiones anteriores, el control de inicio de aplicaciones en "doble salto" requería el uso de la etiqueta `KEYWORDS:Prefer`en Studio. Aún se puede usar la etiqueta `KEYWORDS:Prefer`. Si se han configurado tanto KEYWORDS como el método vPrefer, vPrefer tiene prioridad.

  Para obtener más información, consulte CTX232210, el artículo Aplicaciones en Citrix Virtual Apps and Desktops y la documentación de Citrix Receiver para Windows.

Configurar StoreFront multisitio de alta disponibilidad

January 6, 2020

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 los almacenes. 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 almacenes. Para obtener más información, consulte Configuraciones de almacén multisitio con alta disponibilidad.

Combinación de recursos

De forma predeterminada, StoreFront enumera todas las implementaciones que proporcionan escritorios y aplicaciones a un almacén 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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops configuradas para un almacén concreto, 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 Citrix Virtual Apps and Desktops. 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 almacenes 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 un único almacén.

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 al almacén. 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 el almacén, 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 quiere permitir que los usuarios accedan a las mismas aplicaciones desde almacenes 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 el almacén 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 almacenes 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 Configurar 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 hayan 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 Citrix Gateway

Si ha configurado distintos dispositivos Citrix 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 un almacén. Por ejemplo, si crea un almacén que combina los recursos de dos ubicaciones geográficas, cada una con un dispositivo Citrix 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 redirige 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 Citrix Gateway más adecuado para cada una de las implementaciones. Con esta configuración, las conexiones de los usuarios a los recursos se redirigen 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 al almacén.

El enrutamiento óptimo de Citrix Gateway también se puede usar en casos especiales en los que es necesario que los usuarios locales de la red interna inicien sesión en Citrix Gateway para el análisis del punto final. Con esta configuración, los usuarios se conectan al almacén a través del dispositivo Citrix Gateway, pero no es necesario redirigir 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 redirigen directamente y no a través de Citrix Gateway. Tenga en cuenta que también debe configurar una dirección IP concreta para el servidor virtual interno del dispositivo Citrix Gateway. Especifique además una baliza interna inaccesible para que la aplicación Citrix Workspace siempre se conecte a Citrix Gateway, independientemente de la ubicación de red de los usuarios.

Equilibrio de carga del servidor global de Citrix Gateway

StoreFront admite las implementaciones de Citrix Gateway configuradas para equilibrar la carga del servidor global con varios dispositivos configurados con un único FQDN. Para la autenticación de usuario y para redirigir 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 Citrix Gateway.

Para obtener información sobre el equilibrio de carga, consulte Equilibrio de carga con Citrix ADC.

Consideraciones importantes

Si opta por una configuración multisitio de alta disponibilidad para los almacenes, 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 la aplicación Citrix Workspace 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 quiere configurar la sincronización de las suscripciones a aplicaciones de los usuarios entre almacenes de diferentes implementaciones de StoreFront, los almacenes 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.

Instalar, configurar, actualizar y desinstalar

January 31, 2020

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 Citrix Virtual Apps and Desktops a los usuarios, compruebe que el servidor de 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 ningún dominio.
> - StoreFront no se puede instalar en un controlador de dominio.

2. Si aún no está instalado, StoreFront necesita Microsoft .NET Framework, que se puede descargar desde Microsoft. Microsoft .NET 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 de StoreFront.

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

   a) Compruebe que el equilibrio de carga esté habilitado en el dispositivo Citrix ADC.

   b) Para cada servidor de StoreFront, cree servicios de equilibrio de carga HTTP o SSL individuales, según sea adecuado, con el tipo de supervisión de StoreFront.

   c) 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.

   d) Cree un servidor virtual y enlace los servicios al servidor virtual.

   e) En el servidor virtual, configure la persistencia con el método **IP del cliente** o **inserción de cookies**. 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 de StoreFront.

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

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

   Si lo quiere, puede habilitar los siguientes roles y sus dependencias en el servidor de 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

El instalador de StoreFront comprueba que todas las funciones y los roles de servidor precedentes están habilitados.

5. Instalar StoreFront.

   Si quiere que el servidor forme parte de un grupo de servidores, la ubicación de la instalación de StoreFront y los parámetros del sitio web de IIS, la ruta física y los ID del 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, la aplicación Citrix Workspace requiere conexiones HTTPS a los almacenes. Para configurar IIS de modo que se pueda usar un HostBaseURL HTTPS en StoreFront, cree un enlace HTTPS al sitio web predeterminado y vincúlelo al certificado del servidor de StoreFront. Para obtener más información acerca de cómo agregar un enlace HTTPS a un sitio IIS, consulte Proteger la implementación de StoreFront.

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 de 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. Usar la consola de administración de Citrix StoreFront para configurar el servidor

Instalar StoreFront

> **Importante**
>
> 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.

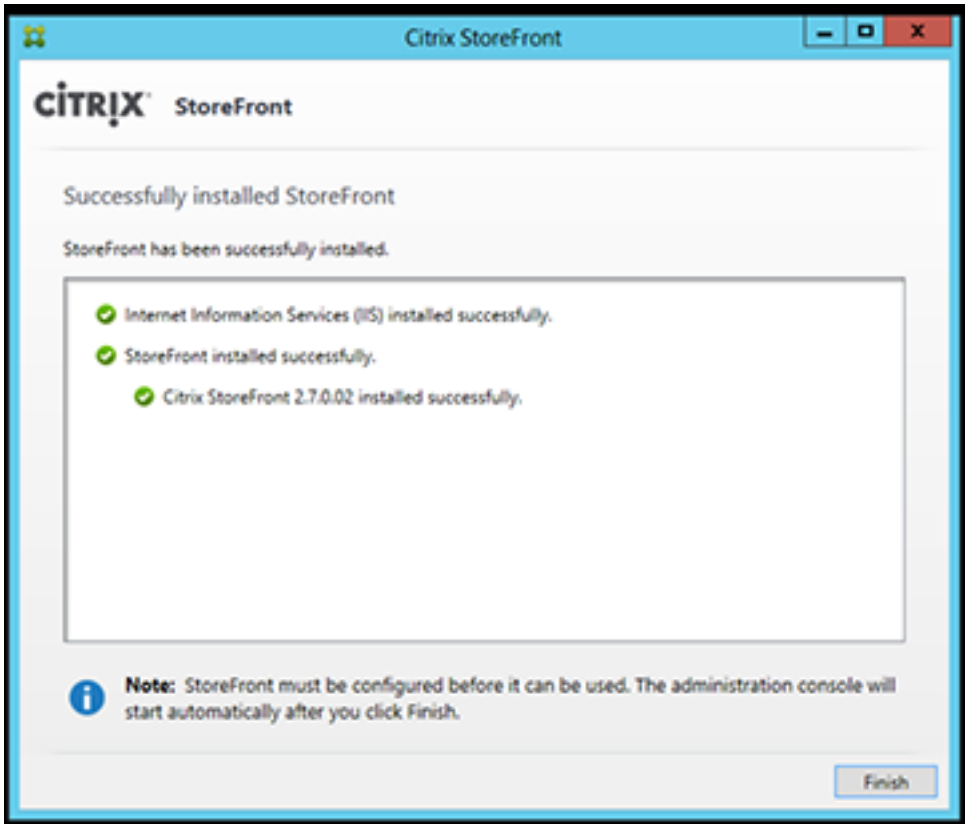
1. Descargue el programa de instalación desde la página de descarga.
2. Inicie sesión en el servidor de StoreFront con una cuenta con permisos de administrador local.
3. Compruebe que Microsoft .NET Framework, requisito necesario, esté instalado en el servidor.
4. Busque CitrixStoreFront-x64.exe y ejecute el archivo como administrador.
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, consulte los requisitos previos y los componentes de StoreFront que se van a instalar 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
   - 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 > .NET Framework, ASP.NET
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**.
    a) Especifique la URL del servidor de StoreFront en el cuadro **URL base**.
    b) En la página **Nombre del almacén**, especifique un nombre para el almacén y haga clic en **Siguiente**.

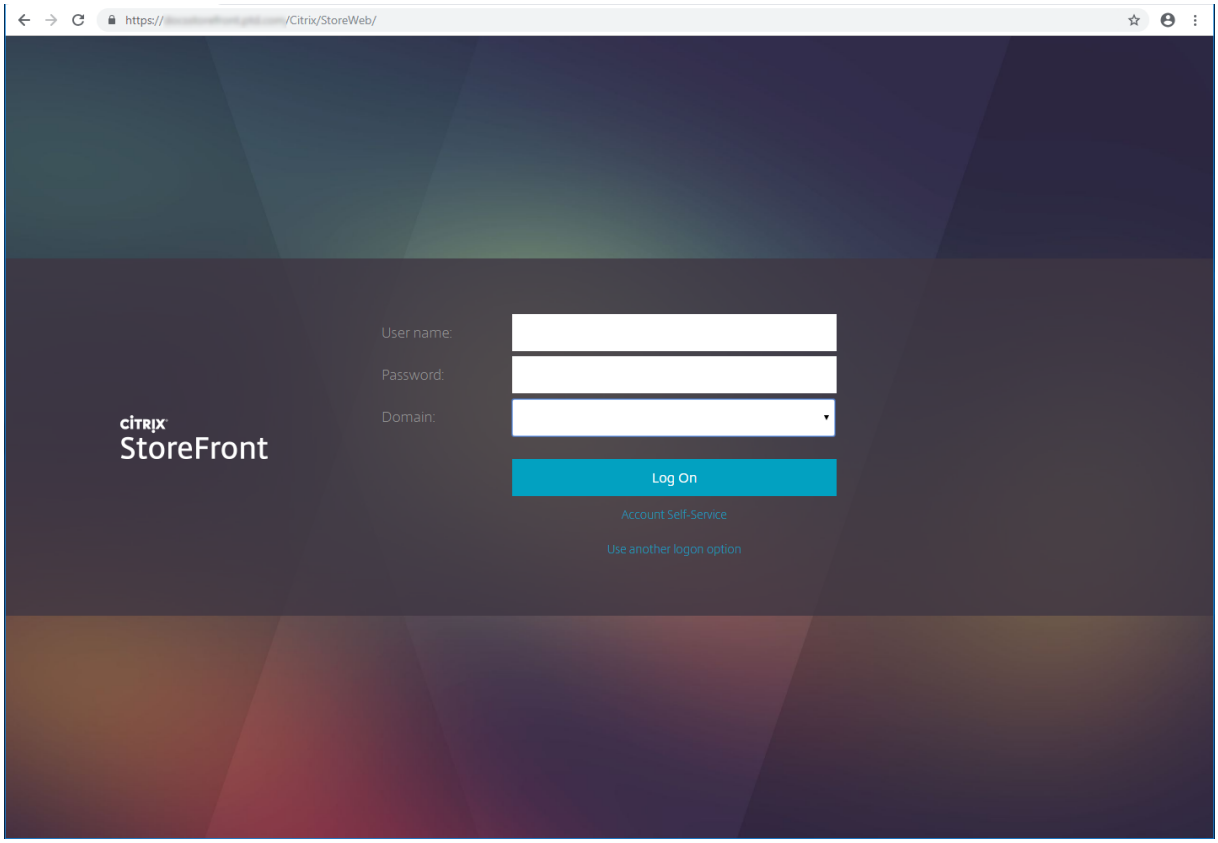
En la página **Delivery Controllers**, indique datos de las implementaciones de Citrix Virtual Apps and Desktops que proporcionan los recursos que quiere ofrecer en el almacén.

1. Establezca el **Tipo de transporte** y el **Puerto**, por ejemplo, HTTP y puerto 80 o HTTPS y puerto 443. A continuación, haga clic en **Aceptar**.
2. En la página **Acceso remoto**, seccione Ninguno. Si utiliza Citrix Gateway, seleccione Sin túnel VPN e indique datos de su puerta de enlace.
3. En la página **Acceso remoto**, seccione Crear. Después de haber creado el almacén, haga clic en **Finalizar**.

Ahora, el almacén está disponible para que los usuarios accedan a él 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 a un sitio de Citrix Receiver para Web para el nuevo almacén. Por ejemplo: `example.net/Citrix/StoreWeb/`. Inicie sesión y accederá a la

nueva interfaz de usuario en la aplicación Citrix Workspace.



Para instalar StoreFront desde un símbolo del sistema

1. Inicie sesión en el servidor de StoreFront con una cuenta con permisos de administrador local.
2. Asegúrese de que se cumplan los requisitos para la instalación de StoreFront antes de instalar StoreFront. Consulte Antes de instalar y configurar para obtener información detallada.
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 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 en el que

se instalará StoreFront. Si quiere que el servidor forme parte de un grupo de servidores, la ubicación de la instalación de StoreFront y los parámetros del sitio web de IIS, la ruta física y los ID del sitio deben ser idénticos en todos los servidores del grupo.

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

Si va a cambiar esta configuración, especifique los argumentos **-WINDOWS_CLIENT** y **-MAC_CLIENT** para copiar los archivos de instalación de Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows y Citrix Receiver para Mac o la aplicación Citrix Workspace para Mac, respectivamente, a la ubicación adecuada en la 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. Los archivos de instalación de Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows y Citrix Receiver para Mac o la aplicación Citrix Workspace para Mac se incluyen en los medios de instalación de Citrix Virtual Apps and Desktops.

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 se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar 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. Haga una copia de seguridad del Registro antes de modificarlo.

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


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

De forma predeterminada, la propiedad **Enabled** está oculta en el registro. 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 mediante el parámetro de Registro, la ausencia de 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 almacenes	Un contador de la cantidad de almacenes que hay en la implementación.
Recuento de servidores en el grupo de servidores	Un contador de la cantidad de servidores que hay en el grupo de servidores.
Recuento de Delivery Controllers por almacén	Lista de valores numéricos que indican la cantidad de Delivery Controllers disponibles para cada almacén que haya en la implementación.
HTTPS habilitado	Cadena que indica si HTTPS (“True” o “False”) está habilitado para la implementación.

Datos	Descripción
Parámetro de HTML5 para Citrix Receiver para web	Lista de las cadenas de texto que indican el parámetro de HTML5 de cada Receiver para web.
Control del espacio de trabajo habilitado para la aplicación Citrix Workspace/Citrix Receiver	Lista de valores booleanos que indican si el “Control del espacio de trabajo” está habilitado (“True” o “False”) en cada sitio de Receiver para web.
Acceso remoto habilitado en el almacén	Lista de las cadenas de texto que indican si el “Acceso remoto” está habilitado (“HABILITADO” o “INHABILITADO”) para cada almacén que haya en la implementación.
Recuento de puertas de enlace	Un contador de la cantidad de puertas de enlace Citrix Gateway configuradas en la implementación.

Citrix Analytics Service

Si es cliente de Citrix Cloud y tiene una implementación local de StoreFront, puede configurar StoreFront para que los datos se envíen a Citrix Analytics Service en Citrix Cloud. Cuando se configura, la aplicación Citrix Workspace y los sitios Citrix Receiver para web a los que se accede desde exploradores compatibles con HTML5 envían eventos de usuario a Citrix Analytics para su procesamiento. Citrix Analytics recoge y agrupa métricas de usuarios, aplicaciones, dispositivos de punto final, redes y datos para proporcionar información completa sobre el comportamiento de los usuarios. Para obtener más información sobre esta función en la documentación de Citrix Analytics, consulte Incorporar sitios de Virtual Apps and Desktops mediante StoreFront.

Para configurar este comportamiento:

- Descargue un archivo de configuración de Citrix Analytics.
- Importe datos de Citrix Analytics en la implementación local de StoreFront mediante PowerShell.

Una vez configurado StoreFront, la aplicación Citrix Workspace puede enviar datos desde almacenes StoreFront cuando Citrix Analytics Service lo solicite.

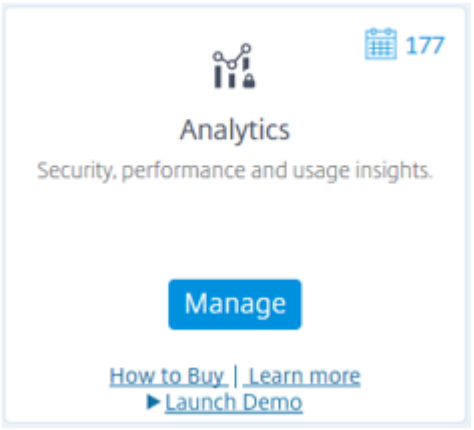
> **Importante:**
>
> La implementación de StoreFront debe poder ponerse en contacto con las siguientes direcciones en el puerto 443 para que esta función se ejecute correctamente y consuma los servicios de Citrix

> Cloud:
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

Descargue el archivo de configuración de Citrix Analytics

> **Importante:**
>
> Se requiere un archivo de configuración que contiene información confidencial para la configuración inicial. Mantenga el archivo seguro después de la descarga. No comparta este archivo con nadie fuera de su organización. Después de la configuración, puede eliminar este archivo. Si necesita volver a aplicar la configuración en otro equipo, puede descargar el archivo de nuevo desde la consola de administración de Citrix Analytics Service.

1. Inicie sesión en Citrix Cloud (`https://citrix.cloud.com/`) con una cuenta de administrador.
2. Seleccione un cliente de Citrix Cloud.
3. Para abrir la consola de administración de servicios de Citrix Analytics, haga clic en **Administrar**.



4. En la consola de administración de servicios de Citrix Analytics, seleccione **Settings > Data Sources**.
5. En la tarjeta Virtual Apps and Desktops, seleccione el icono de menú (⋮) y, luego, **Connect StoreFront deployment**.
6. En la página Connect StoreFront Deployment, seleccione **Download File** para descargar el archivo *StoreFrontConfigurationFile.json*.

Archivo de configuración de ejemplo

```
1 {
```



```
2
3   "customerId": "<yourcloudcustomer>",
4   "enablementService": " https://api.analytics.cloud.com /casvc/<
       yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
       deviceid>/dsconfigdata",
5   "cwsServiceKey": "PFJTPn ..... .. T4=",
6   "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
       yourcloudcustomer>/ctxana/v1/cas/storefront/config",
7   "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
8   "name": "CASSingleTenant"
9  }
```

donde

customerId es el identificador único del cliente actual de Citrix Cloud.

cwsServiceKey es una clave única que identifica la cuenta de cliente actual de Citrix Cloud.

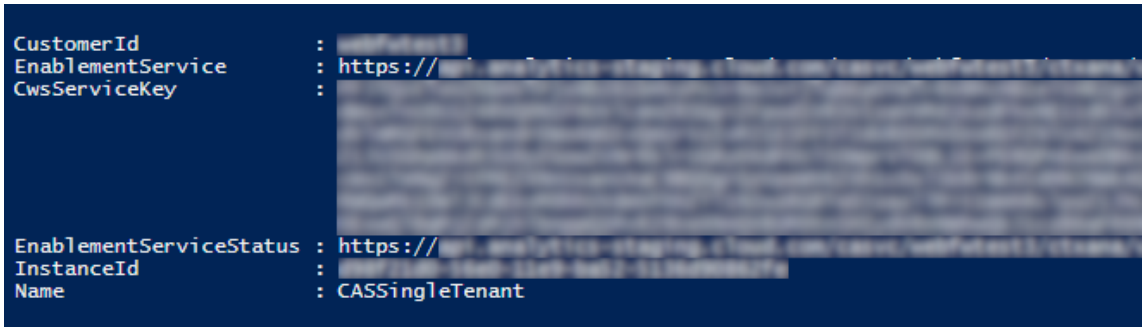
instanceID es un ID generado que se utiliza para firmar (proteger) las solicitudes realizadas desde la aplicación Citrix Workspace para Citrix Analytics. Si registra varios servidores o grupos de servidores de StoreFront con Citrix Cloud, cada uno tiene un instanceID único.

Importar datos de Citrix Analytics en su implementación de StoreFront

1. Copie el archivo *StoreFrontConfigurationFile.json* en una carpeta adecuada del servidor local de StoreFront (o en un servidor de un grupo de servidores de StoreFront). Los siguientes comandos dan por supuesto que el archivo se guarda en el escritorio.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Ejecute los comandos siguientes:

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

4. Este comando devuelve una copia de los datos importados y los muestra en la consola de PowerShell.



> **Nota:**
>
> Los servidores locales de StoreFront, que están instalados en Windows Server 2012 R2, pueden requerir que los componentes de software del runtime de C++ se instalen manualmente para que puedan registrarse con el servicio CAS. Si StoreFront se instala durante la instalación de Citrix Virtual Apps and Desktops, este paso no es necesario porque el metainstalador de CVAD ya instala los componentes del runtime de C++. Si StoreFront se instala solamente con el metainstalador CitrixStoreFront-x64.exe y sin el runtime de C++, es posible que no se registre con Citrix Cloud después de importar el archivo de configuración del servicio CAS.

Propagar datos de Citrix Analytics en un grupo de servidores de StoreFront

Si realiza estas acciones en un grupo de servidores de StoreFront, debe propagar los datos importados de Citrix Analytics en todos los miembros del grupo de servidores. Este paso no es necesario en implementaciones con un solo servidor de StoreFront.

Para propagar los datos, utilice uno de los siguientes métodos:

- Utilice la consola de administración de StoreFront.
- Utilice el cmdlet de PowerShell **Publish-STFServerGroupConfiguration**.

Comprobar el ID del grupo de servidores de StoreFront

Para comprobar si la implementación se ha registrado correctamente en Citrix Analytics Service, puede usar PowerShell para detectar ServerGroupID en la implementación.

1. Inicie sesión en el servidor de StoreFront o en un servidor de StoreFront del grupo de servidores.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Ejecute los comandos siguientes:

```
1 $WebConfigPath = ”C:\Program Files\Citrix\Receiver StoreFront\
     Framework\FrameworkData\Framework.xml”
2 $XMLObject = (Get-Content $WebConfigPath) -as [Xml]
3 $XMLObject.framework.properties.property
```


Por ejemplo, estos comandos generan resultados como los siguientes:

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

Dejar de enviar datos a Citrix Analytics desde StoreFront

1. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
2. Ejecute los comandos siguientes:

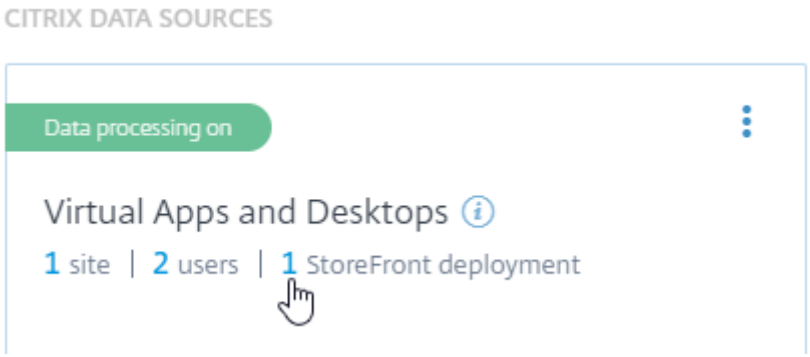
   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

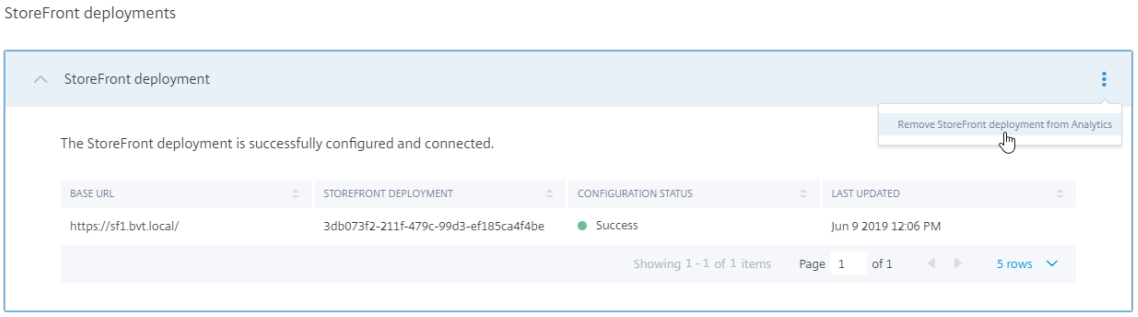
   Get-STFCasConfiguration no devuelve nada si los datos importados anteriormente de Citrix Analytics se han eliminado correctamente.
3. Si realiza estas acciones en un grupo de servidores de StoreFront, propague el cambio y elimine los datos importados de Citrix Analytics de todos los miembros del grupo de servidores. En un servidor del grupo de servidores, ejecute el siguiente comando:

   ```
   Publish-STFServerGroupConfiguration
   ```
4. En cualquier otro miembro del grupo de servidores, ejecute el siguiente comando para confirmar que la configuración de Citrix Analytics se ha eliminado correctamente de todos los servidores del grupo:

   ```
   Get-STFCasConfiguration
   ```
5. Inicie sesión en Citrix Cloud (`https://citrix.cloud.com/`) con una cuenta de administrador.
6. Seleccione un cliente de Citrix Cloud.
7. Para abrir la consola de administración de servicios de Citrix Analytics, haga clic en **Administrar**.
8. En la consola de administración de servicios de Citrix Analytics, seleccione **Settings > Data Sources**.
9. En la tarjeta Virtual Apps and Desktops, seleccione el recuento de implementaciones de StoreFront.



10. Para identificar la implementación de StoreFront que quiere eliminar, haga referencia a la URL base de su host y a ServerGroupID.
11. En el menú (⊠), seleccione **Remove StoreFront deployment from Analytics**.



> **Nota:**
>
> Si quita la configuración del servidor, pero no de Citrix Analytics, la entrada de la implementación de StoreFront permanece en Citrix Analytics, pero no recibe datos de StoreFront. Si quita la configuración solamente de Citrix Analytics, la entrada de la implementación de StoreFront se vuelve a agregar en el siguiente reciclaje del grupo de aplicaciones (tiene lugar al restablecer IIS o automáticamente cada 24 horas).

Configurar StoreFront para que use un proxy web para ponerse en contacto con Citrix Cloud y registrarse con Citrix Analytics

Si StoreFront se coloca en un servidor web host detrás de un proxy web, ocurrirá un error en el registro con Citrix Analytics. Si los administradores de StoreFront utilizan un proxy HTTP en su implementación de Citrix, el tráfico de StoreFront asociado a Internet debe pasar a través del proxy web antes de que llegue a Citrix Analytics en la nube. StoreFront no utiliza automáticamente la configuración de proxy del SO de alojamiento; se requiere una configuración adicional para indicar al almacén que envíe el tráfico saliente a través del proxy web. Puede establecer una configuración de proxy <`system.net`> agregando una nueva sección al archivo web.config del almacén. Haga esto para cada almacén del servidor de StoreFront que se utilice para enviar datos a Citrix Analytics.

Método 1: Establecer la configuración del proxy del almacén a través de PowerShell para uno o varios almacenes (recomendado)

La ejecución del script de PowerShell Config-StoreProxy.ps1 automatiza este proceso para uno o varios almacenes e inserta automáticamente XML válido para configurar <system.net>. El script también realiza una copia de seguridad del archivo web.config del almacén en el escritorio del usuario actual, para permitir restaurar el archivo web.config no modificado si es necesario.

> **Nota:**
>
> Ejecutar el script más de una vez puede dar lugar a que se agreguen varias copias del código XML de <system.net>. Cada almacén solo debe tener una entrada para <system.net>. Agregar varias copias impide que la configuración del proxy de almacén funcione correctamente.

1. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
2. Configure `$Stores = @("Store","Store2")` para que incluya los almacenes que quiere configurar con un proxy web.
3. Especifique:
   - una dirección IP, o bien
   - un nombre de dominio completo (FQDN) para el proxy web
4. Ejecute el siguiente comando de PowerShell:

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

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

    [CmdletBinding()]
    param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
        Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
        array]$Stores,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
            string]$ProxyIP,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][
            string]$ProxyFQDN,
         [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][
            Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")
            ][int]$ProxyPort)

    foreach($Store in $Stores)
```



```
17      {
18
19          Write-Host "Backing up the Store web.config file for store
                $Store before making changes..." -ForegroundColor "
               Yellow"
20          Write-Host "`n"
21
22          if(!(Test-Path "$env:UserProfile\desktop$Store"))
23          {
24
25              Write-Host "Creating $env:UserProfile\desktop$Store\
                   directory for backup..." -ForegroundColor "Yellow"
26              New-Item -Path "$env:UserProfile\desktop$Store" -
                   ItemType "Directory" | Out-Null
27              Write-Host "`n"
28           }
29
30
31          Write-Host "Copying c:\inetpub\wwwroot\Citrix$Store\web.
               config to $env:UserProfile\desktop$Store..." -
               ForegroundColor "Yellow"
32          Copy-Item -Path "c:\inetpub\wwwroot\Citrix$Store\web.
               config" -Destination "$env:UserProfile\desktop$Store" -
               Force | Out-Null
33
34          if(Test-Path "$env:UserProfile\desktop$Store\web.config")
35          {
36
37              Write-Host "$env:UserProfile\desktop$Store\web.config
                   file backed up" -ForegroundColor "Green"
38           }
39
40          else
41          {
42
43              Write-Host "$env:UserProfile\desktop$Store\web.config
                   file NOT found!" -ForegroundColor "Red"
44           }
45
46          Write-Host "`n"
47
48          Write-Host "Setting the proxy server to $ProxyAddress for
               Store $Store..." -ForegroundColor "Yellow"
49          Write-Host "`n"
50
```



```
$StoreConfigPath = "c:\inetpub\wwwroot\Citrix$Store\web.config"
$XMLObject = (Get-Content $StoreConfigPath) -as [Xml]

if([string]::IsNullOrEmpty($ProxyFQDN))
{

    $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
 }

else
{

    $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
 }


$XMLObject = (Get-Content $StoreConfigPath) -as [Xml]

# Create 3 elements
$SystemNet = $XMLObject.CreateNode("element","system.net","")
$DefaultProxy = $XMLObject.CreateNode("element","defaultProxy","")
$Proxy = $XMLObject.CreateNode("element","proxy","")
$Proxy.SetAttribute("proxyaddress","$ProxyServer")
$Proxy.SetAttribute("bypassonlocal","true")

# Move back up the XML tree appending new child items in reverse order
$DefaultProxy.AppendChild($Proxy)
$SystemNet.AppendChild($DefaultProxy)
$XMLObject.configuration.AppendChild($SystemNet)

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

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

```
89      }
90
91      Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92      IISReset /RESTART
93  }
94
95
96  Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
        ProxyPort $ProxyPort
97  # OR
98  Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
        $ProxyPort
```

5. Compruebe que C:\inetpub\wwwroot\Citrix\web.config contiene ahora una nueva sección " al final del archivo web.config.

```
1           </dependentAssembly>
2       </assemblyBinding>
3   </runtime>
4   <system.net>
5       <defaultProxy>
6       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
            bypassonlocal="true" />
7       </defaultProxy>
8   </system.net>
9   </configuration>
```

6. Importe los datos de Citrix Analytics tal y como se describe en Importar datos de Citrix Analytics en su implementación de StoreFront.

Método 2: Agregar manualmente una sección `<system.net>` al archivo web.config del almacén

Esto se debe hacer para cada almacén del servidor de StoreFront que se utilice para enviar datos a Citrix Analytics.

1. Haga una copia de seguridad del archivo web.config del almacén y cópielo en otra ubicación, fuera de C:\inetpub\wwwroot\Citrix\web.config.
2. Modifique el siguiente XML con su configuración de proxy mediante una combinación de FQDN y puerto o mediante una combinación de IP y puerto.

   Por ejemplo, mediante una combinación de FQDN y puerto, utilice el siguiente elemento <system.net>:


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

Por ejemplo, mediante una combinación de IP y puerto, utilice el siguiente elemento <system.net>:

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

3. Al final del archivo web.config del almacén, inserte el elemento <system.net> apropiado donde se indica aquí:

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

Insert the <system.net> element here

</configuration>
```

4. Importe los datos de Citrix Analytics tal y como se describe en Importar datos de Citrix Analytics en su implementación de StoreFront.

Actualizar StoreFront

> **Advertencia:**
>
> Al actualizar a StoreFront 1912, todos los sitios de Desktop Appliance de la implementación se quitan automáticamente. Si necesita conservar los sitios de Desktop Appliance, no procese la actualización. Como alternativa, Citrix recomienda usar Desktop Lock y aplicación Citrix Workspace para todos los casos de uso no asociados a un dominio.

La actualización conserva la configuración de StoreFront y deja 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. Por el contrario, desinstalar StoreFront elimina StoreFront y los servicios, sitios, datos de suscripción de aplicaciones (en servidores independientes) y la configuración asociados.

Conviene tener en cuenta lo siguiente

- No se admite la actualización de versiones de los sistemas operativos en un servidor con StoreFront. Citrix recomienda instalar StoreFront en una instalación limpia del sistema operativo.
- No se admite la actualización a la versión más reciente de StoreFront desde una versión antigua que esté en el ciclo Fin de vida. Para obtener más información, consulte CTX200356.
- StoreFront no admite implementaciones de varios servidores que contengan versiones diferentes del producto, por lo que todos los servidores de un grupo de servidores deben actualizarse a la misma versión antes de conceder el acceso a la implementación.
- StoreFront no admite implementaciones de varios servidores con sistemas operativos de servidor diferentes, por lo que todos los servidores de un grupo de servidores deben tener el mismo sistema operativo de servidor de Windows.
- No se admite la actualización simultánea para las implementaciones con varios servidores; los servidores deben actualizarse de forma secuencial.
- Todos los almacenes que utilicen la experiencia de usuario clásica se actualizan para utilizar la experiencia unificada cuando se actualiza a esta versión de StoreFront. Se recomienda informar a los usuarios de la nueva experiencia que introduce la actualización, descrita en Experiencia de usuario unificada. Si ha personalizado la experiencia unificada, las personalizaciones se conservan al actualizar StoreFront a esta versión. Compruebe que la apariencia de las personalizaciones sigue siendo la adecuada con la nueva experiencia unificada.
- Antes de que se ejecute la actualización de StoreFront, se realizan algunas comprobaciones previas a la actualización. Si falla alguna comprobación previa a la actualización, la actualización no se inicia y se le notifica de los errores. Su instalación de StoreFront no cambia. Tras haber corregido la causa de los fallos, vuelva a ejecutar la actualización.
- Si se produce un error en la propia actualización de StoreFront, es posible que la instalación existente de StoreFront pierda su configuración inicial. Restaure la instalación de StoreFront a un estado funcional y vuelva a ejecutar la actualización. Para restaurar StoreFront a un estado

funcional, tenga en cuenta los siguientes enfoques:
  - Restaurar la instantánea de VM que creó antes de la actualización
  - Importar la configuración de StoreFront que exportó antes de la actualización (consulte Exportar e importar la configuración de StoreFront)
  - Seguir los consejos de la solución de problemas indicados en Solucionar problemas de actualización de StoreFront
- Cualquier error de actualización de StoreFront que se produzca desde el metainstalador de Citrix Virtual Apps and Desktops queda notificado en un cuadro de diálogo, con un enlace al registro de errores correspondiente.

Prepararse para la actualización

Antes de iniciar la actualización, se recomienda seguir estos pasos para evitar errores en la actualización:

- Planifique su estrategia de seguridad antes de actualizar la versión.
- Cierre todas las demás aplicaciones del servidor de StoreFront.
- Cierre la consola de administración de StoreFront.
- Cierre todas las ventanas de línea de comandos y de PowerShell.
- Cierre todas las carpetas relacionadas con StoreFront, como C:\inetpub\wwwroot\Citrix\Store y C:\inetpub\wwwroot\Citrix\StoreWeb. Esto evita que el Explorador de Windows las bloquee de forma exclusiva.
- Antes de actualizar un servidor, reinícielo para asegurarse de que no haya bloqueos exclusivos en los archivos o carpetas de StoreFront (el hecho de reiniciar el proceso explorer, por ejemplo, al cerrar todas las instancias del Explorador de Windows, *no* es suficiente).
- Ejecute la actualización inmediatamente sin iniciar ningún otro programa en el servidor.
- Actualice el servidor con una cuenta de administrador, sin ninguna instalación en curso y con el mínimo de aplicaciones.

Actualizar un servidor de StoreFront independiente

1. Desconecte a los usuarios de la implementación de StoreFront para impedir que accedan a los servidores mientras la actualización tiene lugar. De esta manera, el instalador puede acceder a todos los archivos de StoreFront durante la actualización. Si el instalador no puede acceder a los archivos, estos no se reemplazan y la actualización no se produce, lo que provoca la eliminación de la configuración existente de StoreFront.
2. Haga una copia de seguridad del servidor mediante la creación de una instantánea de VM.
3. Exportar la configuración existente de StoreFront (recomendado).
4. Ejecute el archivo de instalación de esta versión de StoreFront.

Para actualizar un grupo de servidores de StoreFront

La actualización de grupos de servidores de StoreFront conlleva el uso de uno de los servidores para quitar los demás servidores del grupo. Los servidores eliminados conservan la configuración relacionada con el grupo, lo que puede impedir que se unan a un nuevo grupo de servidores. Antes de que puedan volver a utilizarse para crear grupos de servidores o como servidores de StoreFront independientes, deben restablecerse a los valores predeterminados de fábrica o reinstalar StoreFront en ellos.

Antes de actualizar un grupo de servidores:

- Haga copias de seguridad de todos los servidores del grupo mediante la creación de instantáneas de VM. Esto le permite volver rápidamente a un grupo de servidores funcional de tres nodos si la actualización no se realiza según lo planeado.
- Exportar la configuración existente de StoreFront (recomendado). Exporte solamente la configuración del grupo de servidores desde un servidor. Siempre que haya propagado todos los cambios entre ellos, todos los servidores de un grupo de servidores conservan copias idénticas de la configuración. Esta copia de seguridad le permite crear fácilmente otro grupo de servidores.

Ejemplo 1: Actualizar un grupo de servidores de StoreFront de tres nodos durante el tiempo de inactividad programado por mantenimiento

Esto describe la actualización de un grupo de servidores de StoreFront de tres servidores, A, B y C, durante el tiempo de inactividad programado.

1. Para inhabilitar el acceso de los usuarios al grupo de servidores, inhabilite la URL de equilibrio de carga. Esto impide que los usuarios se conecten a la implementación durante la actualización.
2. Utilice el servidor A para quitar los servidores B y C del grupo.

   Los servidores B y C se quedan “huérfanos” del grupo de servidores.
3. Para actualizar el servidor A, ejecute el archivo de instalación de esta versión de StoreFront.
4. Compruebe que el servidor A se ha actualizado correctamente.
5. En los servidores B y C, desinstale la versión actualmente instalada de StoreFront y, luego, instale la nueva versión de StoreFront.
6. Una los servidores B y C al servidor actualizado A para crear un grupo de servidores actualizado. Este grupo de servidores consta de un servidor actualizado (A) y dos servidores recién instalados (B y C).

   El proceso de Unirse a un grupo de servidores existente propaga automáticamente todos los datos de configuración y de suscripción a los nuevos servidores B y C.

7. Compruebe que todos los servidores funcionan correctamente.
8. Para habilitar el acceso de los usuarios al grupo de servidores actualizado, habilite la URL de equilibrio de carga.

Ejemplo 2: Actualizar un grupo de servidores de StoreFront de tres nodos sin tiempo de inactividad programado

Esto describe la actualización de un grupo de servidores de StoreFront de tres servidores, A, B y C, sin tiempo de inactividad programado.

Antes de actualizar un grupo de servidores:

1. Exporte los datos de suscripción del servidor A mediante **Export-STFStoreSubscriptions**. Esta copia de seguridad es necesaria porque los servidores se restablecen a sus valores de fábrica más adelante en el proceso, lo que elimina los datos de suscripción y de configuración. Consulte Administrar datos de suscripción a un almacén.
2. Para inhabilitar el acceso de los usuarios al servidor C, inhabilite el servicio del equilibrador de carga que representa el servidor C. Esto impide que los usuarios se conecten al servidor C durante la actualización. Mantenga habilitado el servicio del equilibrador de carga que representan los servidores A y B, de modo que los usuarios puedan seguir utilizándolos.
3. Utilice el servidor A para quitar el servidor C del grupo.
   Los servidores A y B siguen ofreciendo acceso a los recursos de sus usuarios. El servidor C se ha quedado huérfano del grupo de servidores, y se han restablecido sus valores de fábrica.
4. Restablezca el servidor huérfano C a sus valores predeterminados de fábrica mediante **Clear-STFDeployment**.
5. Importe la configuración de StoreFront que exportó antes al servidor C mediante **Import-STFConfiguration**.
6. Para actualizar el servidor C, ejecute el archivo de instalación de esta versión de StoreFront. Ahora el servidor C tiene una configuración idéntica a la del grupo de servidores anterior y se actualiza a una nueva versión de StoreFront.
7. Importe los datos de suscripción que exportó antes al servidor C. *No* es necesario repetir este paso más adelante. Solamente un servidor necesita una copia de los datos de suscripción para propagarlos a los demás servidores que se unan al grupo.
8. Repita los pasos del 2 al 6 con el servidor B. Durante este tiempo, solo el servidor A ofrece a los usuarios acceso a los recursos. Por lo tanto, es mejor hacer este paso durante períodos de poca actividad, donde se espere que la carga en el grupo de servidores de StoreFront sea mínima.
9. Una el servidor B al servidor C mediante el proceso de Unirse a un grupo de servidores existente. Esto proporciona una implementación de un solo servidor en la versión actual de StoreFront

(servidor A) y un nuevo grupo de servidores de dos nodos en la nueva versión de StoreFront (servidores B y C).

10. Habilite los servicios del equilibrador de carga para el servidor B y C de modo que puedan tomar el relevo del servidor A.
11. Inhabilite el servicio del equilibrador de carga para el servidor A de modo que los usuarios se dirijan a los servidores recién actualizados B y C.
12. Repita los pasos del 2 al 6 con el servidor A.
    El proceso de actualización del grupo de servidores se ha completado. Los servidores A, B y C tienen datos de configuración y de suscripción idénticos al del grupo original.

> **Nota:**
>
> Durante el breve período en que el servidor A es el único servidor accesible, se pueden perder suscripciones (paso 9). Esto puede provocar que el nuevo grupo de servidores tenga una copia ligeramente obsoleta de la base de datos de suscripción después de la actualización y que se pierdan los nuevos registros de suscripción.
>
> Esto no tiene ningún impacto funcional porque los datos de suscripción no son esenciales para que los usuarios puedan iniciar sesión e iniciar recursos. Sin embargo, los usuarios tendrían que volver a suscribirse a un recurso después de que el servidor A se haya restablecido a sus valores de fábrica y se haya unido al grupo recién actualizado. Aunque es poco probable que se pierdan bastantes registros de suscripción, es una consecuencia posible de la actualización en vivo de un entorno de producción de StoreFront sin tiempo de inactividad.

Configurar StoreFront

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

- Cree una 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 de StoreFront, puede agregar más servidores al grupo en cualquier momento para aumentar la capacidad de la implementación.
- Unirse 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 servidor, necesita acceso a un servidor existente de la implementación. Citrix no recomienda más de 6 servidores en cada grupo de servidores.

Desinstale StoreFront

Además del producto en sí, la desinstalación de StoreFront conlleva la eliminación del servicio de autenticación, los almacenes, los sitios de Citrix Receiver para Web, las direcciones URL de XenApp Services y sus configuraciones asociadas. El servicio de suscripción de almacenes que contiene los datos de suscripción a aplicaciones de los usuarios también se elimina. En implementaciones de un solo servidor, 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 eliminarán del servidor cuando se desinstala StoreFront.

1. Inicie sesión en el servidor de StoreFront con una cuenta con permisos de administrador local.
2. Cierre la consola de administración de StoreFront si está abierta.
3. Cierre las sesiones de PowerShell que se hayan utilizado para administrar StoreFront a través de su SDK de PowerShell.
4. En la pantalla de **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**.
5. 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.
6. En el cuadro de diálogo **Desinstalar Citrix StoreFront**, haga clic en **Sí**. Cuando termine la desinstalación, haga clic en **Aceptar**.

Crear una implementación

March 2, 2020

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 de 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.
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, la aplicación Citrix Workspace requiere conexiones HTTPS a los almacenes. 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 Configurar grupos de servidores.

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

5. En la página **Nombre del almacén**, especifique un nombre para el almacén. Indique asimismo si permitir el acceso solo a usuarios no autenticados (anónimos) y haga clic en **Siguiente**.

   Los almacenes de StoreFront combinan escritorios y aplicaciones, y los ponen a disposición de los usuarios. Los nombres de los almacenes aparecen en la aplicación Citrix Workspace, en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido de cada almacén.

6. En la página **Delivery Controllers**, indique la infraestructura que ofrece los recursos que estarán disponibles en el almacén. Para agregar escritorios y aplicaciones al almacén, lleve a cabo el procedimiento descrito en Agregar recursos de Citrix Virtual Apps and Desktops al almacén. Puede configurar almacenes para proporcionar recursos desde cualquier combinación de implementaciones de Citrix Virtual Apps and Desktops. Repita los procedimientos tantas veces como sea necesario para agregar todas las implementaciones que proporcionan recursos al almacén.

7. Una vez que haya agregado al almacén todos los recursos necesarios, en la página **Delivery 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.

   - Para que el almacén 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 al almacén.
   - Para que solo los recursos entregados mediante Citrix Gateway estén disponibles en el almacén, seleccione **Permitir acceso solo a los recursos entregados mediante StoreFront (sin túnel VPN)**. Los usuarios inician sesión en Citrix Gateway con ICAproxy o una VPN sin cliente (cVPN), y no necesitan usar el plug-in de Citrix Gateway para establecer una VPN completa.

- Para que el almacén 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 plug-in de Citrix Gateway para establecer el túnel VPN.

Al habilitar el acceso remoto al almacén, el método de autenticación **PassThrough desde Citrix Gateway** se habilita automáticamente. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes.

9. Si ha habilitado el acceso remoto, la lista **Dispositivos Citrix Gateway** contiene las implementaciones a través de las que los usuarios pueden acceder al almacén. Para agregar una implementación de Citrix Gateway a esta lista, siga el procedimiento correspondiente descrito en Ofrecer acceso remoto al almacén a través de un dispositivo Citrix Gateway. Repita el procedimiento anterior para agregar tantas implementaciones como sea necesario.
10. En la lista **Dispositivos Citrix Gateway**, seleccione las implementaciones a través de las cuales los usuarios pueden acceder al almacén. Si habilita el acceso a través de varias implementaciones, especifique el **dispositivo predeterminado** que se utilizará para acceder al almacén. Haga clic en **Siguiente**.
11. En la página **Configurar métodos de autenticación**, seleccione los métodos que utilizarán los usuarios para autenticarse y acceder al almacén, 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 los almacenes.
    - **Autenticación SAML:** Los usuarios se autentican en un proveedor de identidades y su sesión se inicia automáticamente cuando acceden a sus almacenes.
    - **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 los almacenes.
    - **Tarjeta inteligente:** Los usuarios se autentican con tarjetas inteligentes y números PIN cuando acceden a los almacenes.
    - **HTTP básica:** Los usuarios se autentican en el servidor web IIS del servidor de StoreFront.
    - **PassThrough desde Citrix Gateway:** Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes. Esta opción se selecciona automáticamente cuando se habilita el acceso remoto. En la página **Configurar validación de contraseñas**, seleccione los Delivery Controllers que ofrecen la validación de contraseñas y haga clic en **Siguiente**.
12. En la página **URL de XenApp Services**, configure la dirección URL de XenApp Services para los usuarios que usen PNAgent para acceder a las aplicaciones y los escritorios.
13. Después de crear el almacén, se habilitan opciones adicionales en la consola de adminis-

tración de Citrix StoreFront. Para obtener más información, consulte Configurar y administrar almacenes.

Ahora, el almacén está disponible para que los usuarios accedan a él mediante la aplicación Citrix Workspace, que debe estar configurada con los datos de acceso al almacén. Existen diversas maneras de proporcionar esta información a los usuarios y facilitarles el proceso de configuración. Para obtener más información, consulte Opciones de acceso de los usuarios.

De manera alternativa, los usuarios pueden acceder al almacén 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 al nuevo almacén, aparece al crearlo.

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

Para agregar rápidamente más servidores a la implementación, seleccione la opción Unirse a un grupo de servidores existente al instalar más instancias de StoreFront.

Agregar recursos de Citrix Virtual Apps and Desktops al almacén

Complete los siguientes pasos para que los escritorios y las aplicaciones que proporcionan Citrix Virtual Apps and Desktops estén disponibles en el almacén que usted crea como parte de la configuración inicial del servidor de StoreFront. Se presupone que se han completado los pasos del 1 al 6 del procedimiento “Crear una implementación” en la parte superior de este artículo.

1. En la página **Delivery Controllers**, indique la infraestructura que ofrece los recursos que estarán disponibles en el almacén. Haga clic en **Agregar**.
2. En el cuadro de diálogo Agregar Delivery Controller, especifique un **nombre simplificado** que le ayude a identificar la implementación y seleccione un **tipo** para indicar cómo se proporcionan los recursos disponibles en el almacén. Escriba los valores predeterminados para Citrix Virtual Apps and Desktops. Puede seleccionar XenApp 6.5 como Tipo, pero este producto ha alcanzado el ciclo Fin de vida (EOL) en junio de 2018 y ahora lo cubre el programa de soporte extendido Extended Support Program.
3. Para que los escritorios y las aplicaciones que ofrece Citrix Virtual Apps and Desktops y XenApp 6.5 estén disponibles en el almacén, agregue los nombres o las direcciones IP de sus servidores

a la lista **Servidores**. Puede indicar varios servidores si quiere ofrecer una tolerancia a fallos. Para ello, especifique las entradas por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para los sitios de Citrix Virtual Apps and Desktops, proporcione datos de los Delivery Controllers. En el caso de las comunidades de XenApp 6.5, indique los servidores con 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 TLS (Transport Layer Security), seleccione **HTTPS**. Si selecciona esta opción para servidores Citrix Virtual Apps and Desktops, debe comprobar 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 6.5 mediante 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 servidores Citrix Virtual Apps and Desktops, el puerto especificado debe ser el puerto que Citrix XML Service utilice.
6. Si utiliza el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores de XenApp 6.5, 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.
7. Haga clic en **Aceptar**. Puede configurar almacenes para proporcionar recursos desde cualquier combinación de implementaciones de Citrix Virtual Apps and Desktops. Para agregar más sitios de Citrix Virtual Desktops o comunidades de Citrix Virtual Apps, repita el procedimiento anterior. Después de agregar todos los recursos necesarios al almacén, vuelva al paso 7 del procedimiento "Crear una nueva implementación" en la parte superior de este artículo.

Ofrecer acceso remoto al almacén a través de un dispositivo Citrix Gateway

Complete los siguientes pasos para configurar el acceso remoto a través de un dispositivo Citrix Gateway al almacén que se crea como parte de la configuración inicial del servidor de StoreFront. Se presupone que ha completado los pasos del 1 al 9 del procedimiento "Crear una implementación" en la parte superior de este artículo.

1. En la página **Acceso remoto** del cuadro de diálogo para crear un almacén en la consola de StoreFront, haga clic en **Agregar**.
2. En el cuadro de diálogo Agregar dispositivo Citrix Gateway, en la página **Parámetros generales**, especifique un **nombre simplificado** para el dispositivo Citrix Gateway que ayudará a los usuarios a identificarlo.

   Los usuarios verán el nombre simplificado que especifique en la aplicación Citrix Workspace, de modo que debe incluir la información relevante en el nombre para ayudarlos a decidir si utilizar esa puerta de enlace o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de Citrix Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.
3. En **URL de Citrix Gateway**, escriba la combinación URL:puerto del servidor virtual de Citrix Gateway de la implementación. Si no especifica ningún puerto, se utiliza el puerto predeterminado `https://` de 443. No es necesario especificar el puerto 443 en la URL.

   Para obtener información sobre cómo crear un nombre de dominio completo (FQDN) para acceder a un almacén de forma interna y externa, consulte Crear un nombre de dominio completo (FQDN) para acceder a un almacén de forma interna y externa.
4. Seleccione el **Uso o rol** de Citrix Gateway a partir de las opciones disponibles.

   - **Autenticación y enrutamiento de HDX:** Citrix Gateway se usará para la autenticación y para el enrutamiento de las sesiones HDX.
   - **Solo autenticación:** Citrix Gateway se usará para la autenticación, no para el enrutamiento de las sesiones HDX.
   - **Solo enrutamiento de HDX:** Citrix Gateway se usará para enrutar sesiones HDX, no para la autenticación.
5. Para todas aquellas implementaciones en las que los recursos que ofrezcan Citrix Virtual Apps and Desktops o XenApp 6.5 estarán disponibles en el almacén, indique las **direcciones URL de Secure Ticket Authority (STA)** de los servidores que ejecutan STA en la página **Secure Ticket Authority**. 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 Citrix Virtual Apps and Desktops o XenApp 6.5. Emite tíquets de sesión en respuesta a las solicitudes de conexión. Esos tíquets de sesión forman la base de la

autenticación y la autorización para acceder a los recursos de Citrix Virtual Apps and Desktops o XenApp 6.5. Utilice la URL de STA correcta (como `HTTPS://` o `HTTP://`), según cómo estén configurados los Delivery Controllers. La dirección URL de STA también debe ser idéntica a la configurada en el dispositivo Citrix Gateway presente en el servidor virtual.

6. Para garantizar que Citrix Virtual Apps and Desktops o XenApp 6.5 mantengan abiertas las sesiones desconectadas mientras la aplicación Citrix Workspace intenta volver a conectarse automáticamente, seleccione **Habilitar fiabilidad de la sesión**.

7. Si ha configurado varios STA y quiere que la fiabilidad de la sesión esté siempre disponible, seleccione **Solicitar tíquets de dos STA, si están disponibles**. StoreFront obtiene tíquets de sesión de dos STA diferentes, con lo que las sesiones de usuario no se interrumpen si un STA deja de estar disponible durante 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**, escriba la **dirección IP del servidor virtual** (VIP) que tenga el dispositivo Citrix Gateway.

   Utilice la dirección IP privada para el servidor virtual de Citrix Gateway, en lugar de la dirección IP pública que está vinculada por NAT a la dirección IP privada. StoreFront suele identificar las puertas de enlace a través de sus URL. Si está utilizando GSLB (equilibrio de carga del servidor global), debe agregar la dirección IP virtual a cada puerta de enlace. Eso permite a StoreFront identificar varias puertas de enlace que utilizan la misma URL (nombre de dominio GSLB) como puertas de enlace distintas. Por ejemplo, el almacén puede tener configuradas tres puertas de enlace con la misma URL, como `https://gslb.domain.com`, pero cada una tendría direcciones IP virtuales únicas configuradas como 10.0.0.1, 10.0.0.2 y 10.0.0.3.

9. Si quiere agregar un dispositivo con Citrix Gateway, seleccione en la lista **Tipo de inicio de sesión** el método de autenticación configurado en el dispositivo para los usuarios de la aplicación Citrix Workspace.

   - 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), se-

leccione el método secundario de autenticación en la lista **Alternativa a tarjeta inteligente**.

10. Si está configurando StoreFront para Citrix Gateway y quiere usar SmartAccess, debe escribir una **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 Citrix Gateway para verificar que las solicitudes recibidas desde Citrix Gateway provienen de ese dispositivo.

    Cuando se utilice GSLB, se recomienda que configure direcciones URL de respuesta únicas para cada una de las puertas de enlace de GSLB. StoreFront debe poder resolver cada una de las URL de respuesta únicas y recurrir a las direcciones IP virtuales privadas configuradas para cada uno de los servidores virtuales de puerta de enlace de GSLB. Por ejemplo, `emeagateway.domain.com`, `usgateway.domain.com` y `apacgateway.domain.com` deben recurrir a la dirección IP virtual de la puerta de enlace correcta.

11. Haga clic en **Crear** para agregar su dispositivo Citrix Gateway a la lista del cuadro de diálogo **Configurar parámetros de acceso remoto**.

    La información sobre la configuración de los dispositivos Citrix Gateway se guarda en el archivo de aprovisionamiento .cr del almacén. Eso permite que la aplicación Citrix Workspace envíe la solicitud de conexión pertinente al comunicarse con los dispositivos por primera vez.

12. Vuelva al paso 10 del procedimiento “Crear una implementación” en la parte superior de este artículo.

Unirse a un grupo de servidores existente

January 6, 2020

Un grupo de servidores puede contener un máximo de cinco servidores. Sin embargo, desde el punto de vista de la capacidad basada en simulaciones, no hay ventaja alguna en crear grupos que contengan más de tres servidores.

Antes de instalar StoreFront en un servidor que está agregando al grupo, asegúrese de que:

- El servidor que está agregando utiliza la misma versión de sistema operativo con la misma configuración regional que el resto de los servidores del grupo. No se admiten los grupos de servidores de StoreFront que contengan combinaciones de versiones de sistema operativo y configuraciones regionales.
- 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.

Si el servidor de StoreFront que está agregando pertenecía anteriormente a un grupo de servidores y se ha eliminado, antes de que pueda agregarse de nuevo, ya sea al mismo grupo de servidores o

a otro, debe restablecer el servidor de StoreFront a un estado predeterminado de fábrica. Consulte Restablecer un servidor a los valores predeterminados de fábrica.

> **Importante:**
>
> 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 al que quiera 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Cualquier cambio de configuración realizado debe propagarse a los demás servidores para garantizar una configuración coherente en toda la implementación.

Restablecer un servidor a los valores predeterminados de fábrica

June 24, 2019

En algunas situaciones, es necesario restablecer una instalación de StoreFront a su estado de instalación inicial. Esto es necesario, por ejemplo, para poder volver a agregar un servidor de StoreFront a

un grupo de servidores.

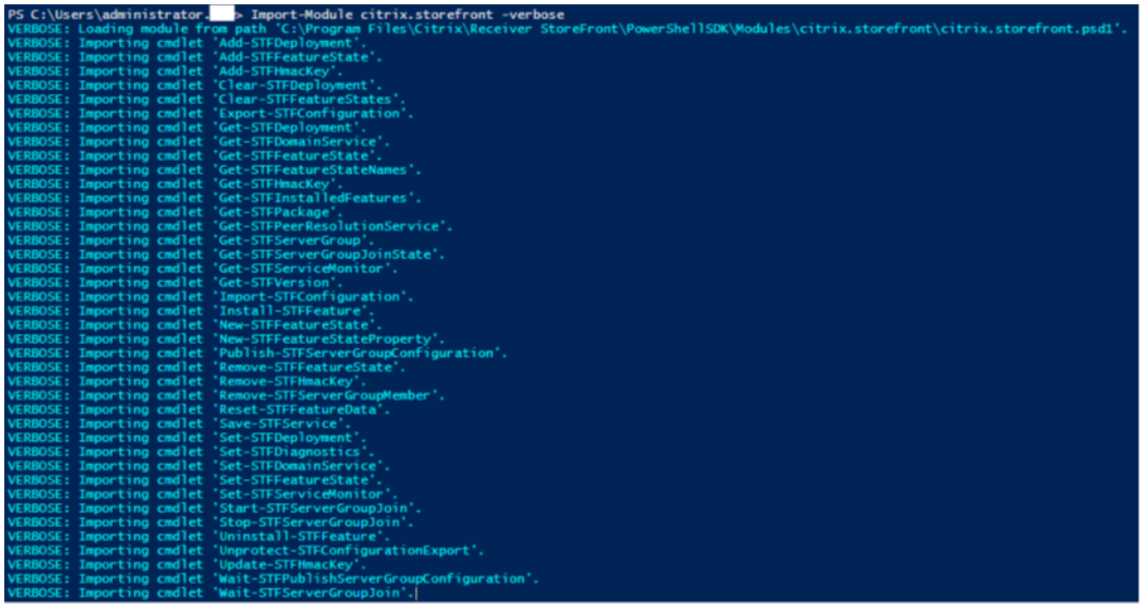
Se puede realizar una desinstalación manual y reinstalación, pero esto requiere más tiempo y puede causar otros problemas inesperados. En su lugar, puede ejecutar el cmdlet de PowerShell **Clear-STFDeployment** para restablecer un servidor de StoreFront a un estado predeterminado de fábrica.

1. Asegúrese de que la consola de administración de StoreFront esté cerrada.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Establezca la ruta de acceso de PowerShell:

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

4. Importe el módulo Citrix StoreFront.

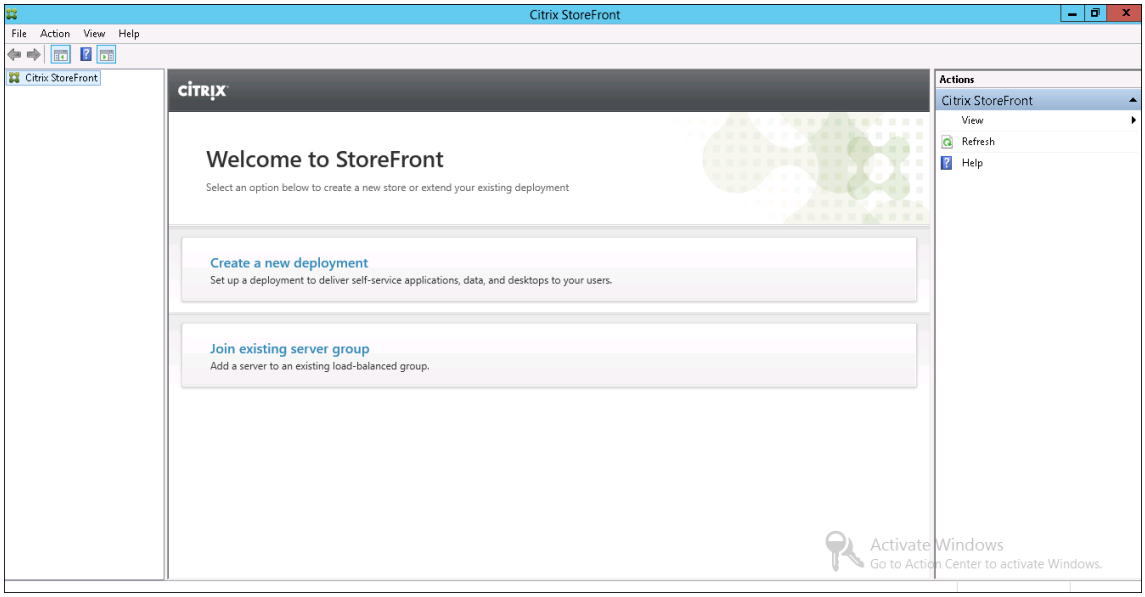
```
Import-Module citrix.storefront -verbose
```



5. Después de importar el módulo, ejecute el comando **Clear-STFDeployment** para restablecer el servidor de StoreFront a los parámetros predeterminados:

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

6. Cuando el comando se haya completado correctamente, abra la consola de administración de StoreFront y asegúrese que se restablezcan todas las configuraciones. Las opciones para **Crear una implementación** o **Incorporarse a un grupo de servidores existente** están disponibles.



Migrar funciones de la Interfaz Web a StoreFront

March 2, 2020

Muchas de las personalizaciones de la Interfaz Web tienen su equivalente en StoreFront y se pueden configurar con 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, permiten a los usuarios elegir	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. **Para inhabilitar 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 el siguiente estilo al archivo style.css: `##searchBtnPhone { display: none; }`
Habilitar actualización	Habilitada de forma predeterminada (actualización del explorador).

Función de la Interfaz Web	Equivalente de StoreFront
Habilitar retorno a la última carpeta	No habilitada de forma predeterminada. Para recordar la carpeta actual y volver a ella al cargar, agregue lo siguiente a script.js: `CTXS.Extensions.afterDisplayHomeScreen = function (){ //check if view was saved last time CTXS.ExtensionAPI.localStorageGetItem(”view”, function (view){ if (view){ // if view was saved, change to it CTXS.ExtensionAPI.changeView(view); } if (view == ”store”){ // if view is store, see if folder was saved CTXS.ExtensionAPI.localStorageGetItem(”folder”, function(folder){ if (folder != ””){ // if folder was saved, change to it CTXS.ExtensionAPI.navigateToFolder(folder); } }); } // set up monitoring of folder CTXS.Extensions.onFolderChange = function(folder){ CTXS.ExtensionAPI.localStorageSetItem(”folder”, folder); } ; // set up monitoring of view CTXS.Extensions.onViewChange = function(newview){ // don’t retain search or appinfo views // instead, remember parent view. if ((newview != ”appinfo”)&&(newview != ”search”)){ CTXS.ExtensionAPI.localStorageSetItem(”view”, newview); } } ; }); } ;`
Habilitar sugerencias	La aplicación Citrix Workspace utiliza muy poco los textos de ayuda, ya que está orientada tanto a los dispositivos táctiles como a los que no son táctiles. Puede agregar textos de ayuda mediante scripts personalizados.

Función de la Interfaz Web	Equivalente de StoreFront
Vista de iconos, Vista de árbol, Vista de detalles, Vista de lista, Vista de grupo, Definir vista predeterminada, (sin gráficos) Vista de iconos, (sin gráficos) Vista de lista, (sin gráficos) Vista predeterminada	La aplicación Citrix Workspace 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 Especificar diferentes vistas de aplicaciones y escritorios.
Interfaz de usuario de ficha única, Interfaz de usuario por fichas (ficha Aplicación, ficha Escritorio, ficha Contenido, (orden de las fichas))	De forma predeterminada, la interfaz de usuario de la aplicación Citrix Workspace está organizada en fichas, con aplicaciones y contenido en una ficha y escritorios en la otra. También existe la ficha optativa **Favoritos**.
Logotipo 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'); }`

Función de la Interfaz Web	Equivalente de StoreFront
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 con clics: `var doneClickThrough = false; // Before web login CTXS.Extensions. beforeLogon = function (callback){ doneClickThrough = true; CTXS. ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for \<a href=” http://www.WWc.com” target=”_blank ”\>WWCo Employees”, okButtonText: ” Accept”, okAction: callback }); } ; // Before main screen (for native clients)CTXS.Extensions. beforeDisplayHomeScreen = function (callback){ if (!doneClickThrough){ CTXS.ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for WWCo Employees”, okButtonText: ”Accept”, okAction: callback }); } else { callback(); } } ;`

Función de la Interfaz Web	Equivalente de StoreFront
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 pantalla de aplicación, mensaje de sistema de pantalla de la aplicación	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; } ** Example static content using a script: **\$('\##customBottom'). html("Welcome to ACME");`

Función de la Interfaz Web	Equivalente de StoreFront
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, porque 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.

Configurar grupos de servidores

January 6, 2020

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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás 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 de 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.

Agregar un servidor a un grupo de servidores

Utilice la tarea Agregar servidor para obtener un código de autorización que le permita unir un servidor de 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 Unirse a un grupo de servidores existente. Consulte el apartado *Escalabilidad* incluido en Planificar una implementación de StoreFront para evaluar la cantidad necesaria de servidores en el grupo.

Eliminar 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.

Para poder volver a agregar un servidor de StoreFront eliminado anteriormente, ya sea al mismo grupo de servidores o a otro, debe restablecerlo al estado predeterminado de fábrica. Consulte Restablecer un servidor a los valores predeterminados de fábrica.

Propagar 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. La propagación de la información de configuración se inicia manualmente para que pueda mantener el control sobre si quiere y el momento en que quiere actualizar los servidores del grupo con los cambios de configuración. Mientras ejecuta esta tarea, no puede realizar cambios adicionales hasta que todos los servidores del grupo se hayan actualizado.

> **Importante:**
>
> Los cambios realizados en otros servidores del grupo se descartan durante la propagación. Si actualiza la configuración de un servidor, propague los cambios a los demás servidores del grupo para evitar que se pierdan si posteriormente propaga cambios desde otro servidor de la implementación.

La información propagada entre servidores del grupo incluye lo siguiente:

- Contenido de todos los archivos web.config, que contienen la configuración de StoreFront.
- Contenido de `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, como `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` y `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`.
- Contenido de `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`.
- Contenido de `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, como imágenes copiadas y archivos .js de personalización.
- Contenido del almacén de certificados de Citrix Delivery Services, excepto las listas de revocación de certificados (CRL) importadas manualmente. (Para obtener información detallada sobre la distribución de CRL locales, consulte la comprobación de listas de revocación de certificados (CRL)).

> **Nota:**
>
> Los datos de suscripción se sincronizan con los demás servidores, independientemente del mecanismo de propagación de cambios. Se produce automáticamente sin que se inicie la tarea Propagar cambios.

Cambiar la dirección URL base de 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 y de que agregue un enlace HTTPS a la página web predeterminada. Para obtener más información, consulte Proteger la implementación de StoreFront.

Configurar el 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 **Duración de la omisión** si se omiten todos los servidores de un Delivery Controller en particular. El valor predeterminado es 0 minutos.
- **Duración de omisión** 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 elevados para **Duración de la omisión si no hay respuesta** cuando se han configurado muchos Delivery Controllers para un almacén, 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 un almacén 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 un almacén

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

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y haga clic en **Administrar Delivery Controllers** en el panel **Acciones**.

3. Seleccione un Controller, haga clic en **Modificar** y luego en **Parámetros** en la pantalla **Modificar Delivery Controller**.
4. En Parámetros avanzados, haga clic en **Parámetros**.
5. En el cuadro de diálogo Configurar parámetros avanzados:
   a) En la fila **Todas las fechas de omisión de omisión**, haga clic en la segunda columna e ingrese un tiempo, en minutos, para el cual un Delivery Controller se considerará fuera de línea después de que todos sus servidores no respondan.
   b) En la fila **Duración de omisión**, haga clic en la segunda columna e ingrese una hora, en minutos, para la cual un solo servidor se considerará fuera de línea después de que no responda.

Configurar la autenticación y la delegación

January 6, 2020

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

Método	Detalles
Configurar el servicio de autenticación	El servicio de autenticación autentica a los usuarios para Microsoft Active Directory, lo que garantiza que dichos 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 Citrix Virtual Apps and Desktops, y no se pueden establecer relaciones de confianza de Active Directory, puede configurar StoreFront para que use el servicio XML de Citrix Virtual Apps and Desktops en la autenticación de 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.

Método	Detalles
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.

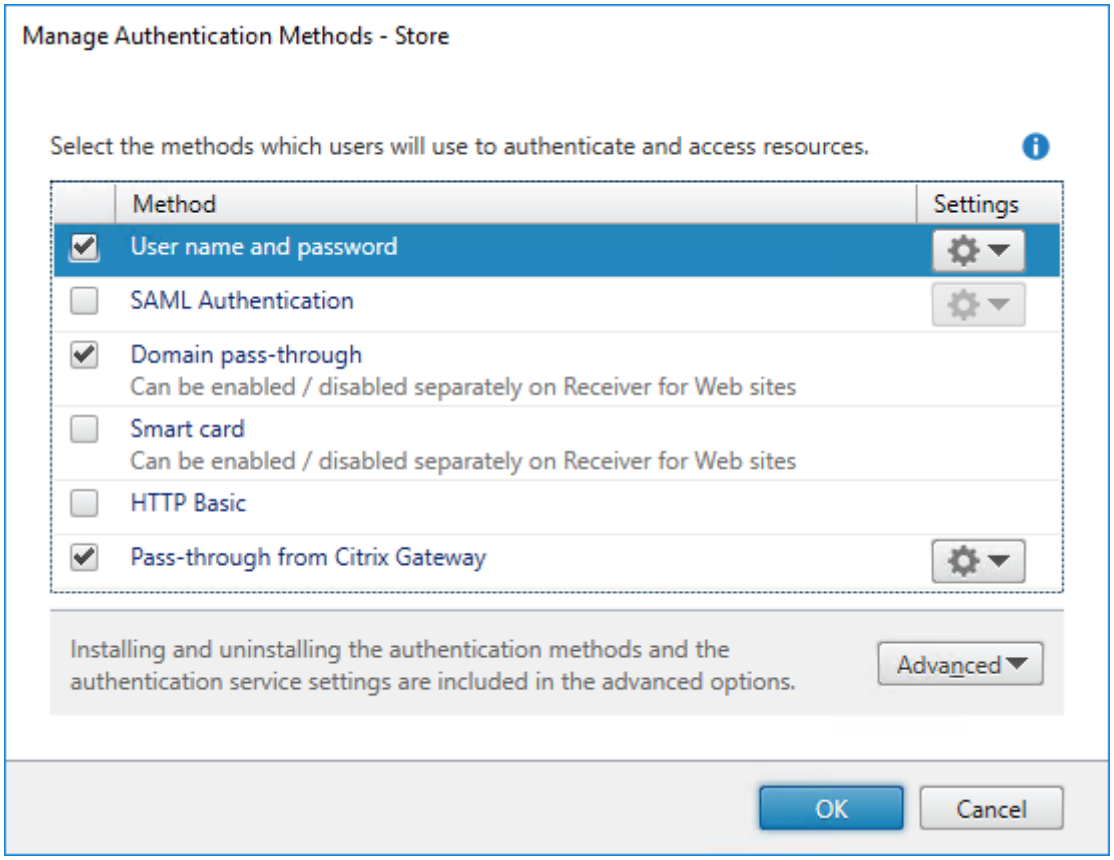
Configurar el servicio de autenticación

January 6, 2020

Administrar 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 de Inicio o Aplicaciones de Windows, busque el icono de Citrix **StoreFront** y haga clic en él.
2. Seleccione el nodo **Almacenes** 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 quiere 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 almacenes.
- Marque la casilla **Autenticación SAML** para permitir la integración en proveedores de identidades SAML. Los usuarios se autentican en un proveedor de identidades y su sesión se inicia automáticamente cuando acceden a sus almacenes. Desde el menú desplegable Parámetros:
  - Seleccione **Proveedor de identidades** para configurar la confianza en 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 los almacenes. Para poder usar esta opción, la autenticación PassThrough debe estar habilitada cuando se instalan Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows en los dispositivos de los usuarios.
- Marque **Tarjeta inteligente** para habilitar la autenticación con tarjeta inteligente. Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a los almacenes.
- Marque **Básica HTTP** para habilitar la autenticación básica HTTP. Los usuarios se autentican en el servidor web IIS del servidor de StoreFront.

- Marque **PassThrough desde Citrix Gateway** para habilitar la autenticación PassThrough desde Citrix Gateway. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes.

Si quiere habilitar la autenticación PassThrough para los usuarios de tarjeta inteligente que acceden a los almacenes a través de Citrix Gateway, use la tarea Configurar autenticación delegada.

Configurar dominios de usuarios de confianza

Utilice la tarea Dominios de confianza para restringir el acceso a los almacenes por parte de usuarios que inician sesión con credenciales de dominio explícitas, ya sea directamente o a través de la autenticación PassThrough desde Citrix 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 “Almacenes” 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 la lista **Nombre de usuario y contraseña > 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 todos los almacenes 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**. Para interrumpir el acceso a los almacenes para las cuentas de usuario en ese dominio, seleccione un dominio de la lista y haga clic en **Quitar**.

   La manera en que se especifica el nombre del dominio determina el formato en el que los usuarios deben introducir sus credenciales. Si quiere 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 quiere 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.

Permitir que los usuarios cambien sus contraseñas

Utilice la tarea **Administrar opciones de contraseña** para permitir que los usuarios de la aplicación Citrix Workspace y de sitios de Receiver para Web que inicien sesión con credenciales de dominio puedan cambiar sus contraseñas. Al crear el servicio de autenticación, la configuración predeterminada impide que los usuarios de la aplicación Citrix Workspace y de los sitios de Citrix Receiver para Web cambien sus contraseñas, incluso aunque estas 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 cambiar las contraseñas, algunas funciones importantes de seguridad se dejan a merced de cualquier persona que pueda acceder a los almacenes a través del 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 los almacenes desde fuera de la red corporativa.

1. Citrix Receiver para Web admite cambios de contraseña por caducidad, así como cambios de contraseña a demanda. Todas las aplicaciones de escritorio de Citrix Workspace admiten el cambio de contraseña a través de Citrix Gateway solo si estas caducan. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. En el panel “Acciones” del panel izquierdo de la consola de administración de Citrix StoreFront, seleccione el nodo **Almacenes** y 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 lo deseen, 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 Configurar el período de notificación sobre caducidad de contraseñas. Solo se admite en Citrix Receiver para Web.
    - Para permitir que los usuarios cambien sus contraseñas solo cuando estas ya hayan caducado, seleccione **Solo cuando caduquen**. Los usuarios que no pueden iniciar sesión porque sus contraseñas han caducado se redirigen al cuadro de diálogo Cambiar contraseña. Este comportamiento se admite en las aplicaciones Citrix Workspace y Citrix Receiver para Web.

> Nota:
>
> Asegúrese de que haya suficiente espacio en disco en los servidores de 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.

- Para evitar que los usuarios cambien sus contraseñas, no seleccione **Permitir a los usuarios cambiar contraseñas**. Si no selecciona esta opción, deberá organizar cómo ofrecer soporte a los usuarios que no puedan acceder a los escritorios y aplicaciones porque sus contraseñas hayan caducado.
- Para evitar que los usuarios cambien sus contraseñas, no seleccione **Permitir a los usuarios cambiar contraseñas**. Si no selecciona esta opción, deberá organizar cómo ofrecer soporte a los usuarios que no puedan acceder a los escritorios y aplicaciones porque sus contraseñas hayan caducado.

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

Preguntas sobre la 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, especifique los usuarios que podrán restablecer contraseñas y desbloquear sus cuentas mediante 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 con un nombre de usuario y una contraseña.

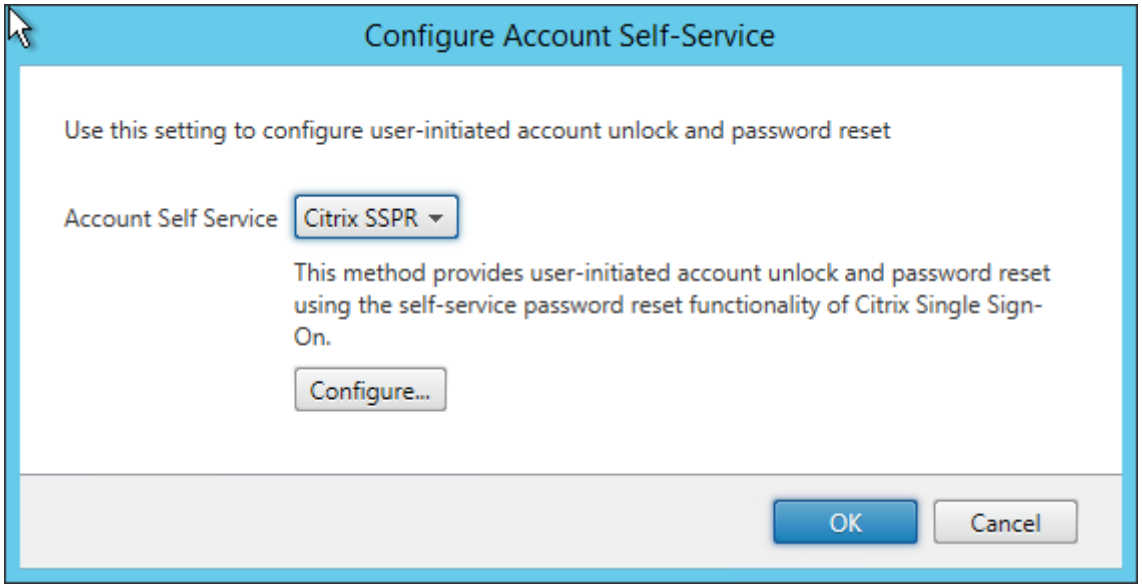
El Autoservicio de restablecimiento de contraseñas no admite el uso de credenciales UPN para el inicio de sesión, tales como `username@domain.com`.

Antes de configurar el Autoservicio de restablecimiento de contraseñas para un almacén, compruebe lo siguiente:

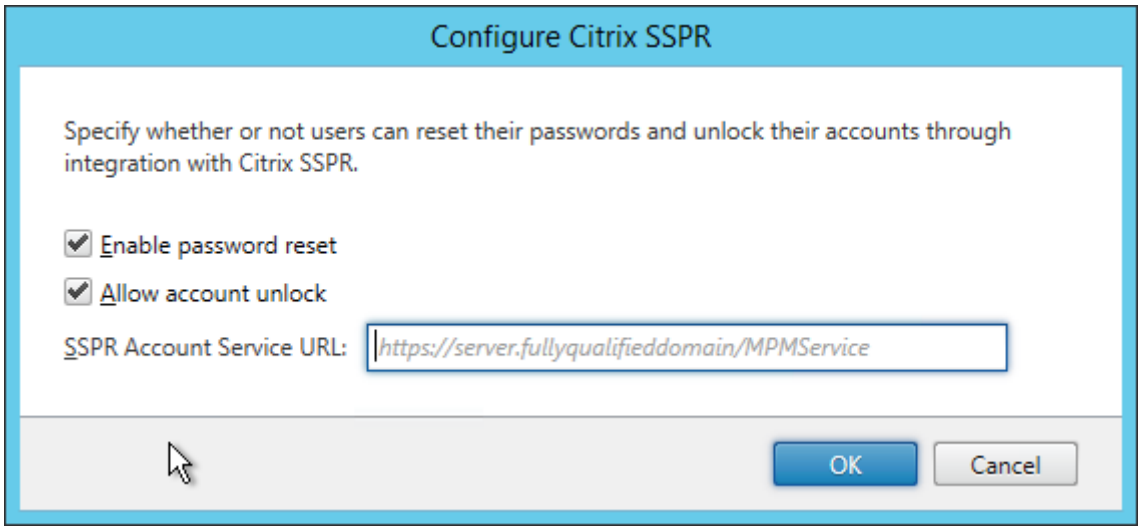
- El almacén está configurado para usar la autenticación con nombre de usuario y contraseña.
- El almacén está configurado para usar solo una instancia de Autoservicio de restablecimiento de contraseñas. Si StoreFront está configurado para utilizar varias comunidades en el mismo dominio o en dominios 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 quiere habilitar la funcionalidad de restablecimiento de contraseñas.
- Debe asociar un almacén de StoreFront a un sitio de Receiver para Web.

Para poder usar el Autoservicio de restablecimiento de contraseñas, hay que instalarlo y configurarlo. Está disponible en los medios de instalación de Citrix Virtual Apps and Desktops. Para obtener información, consulte la documentación de Autoservicio de restablecimiento de contraseñas.

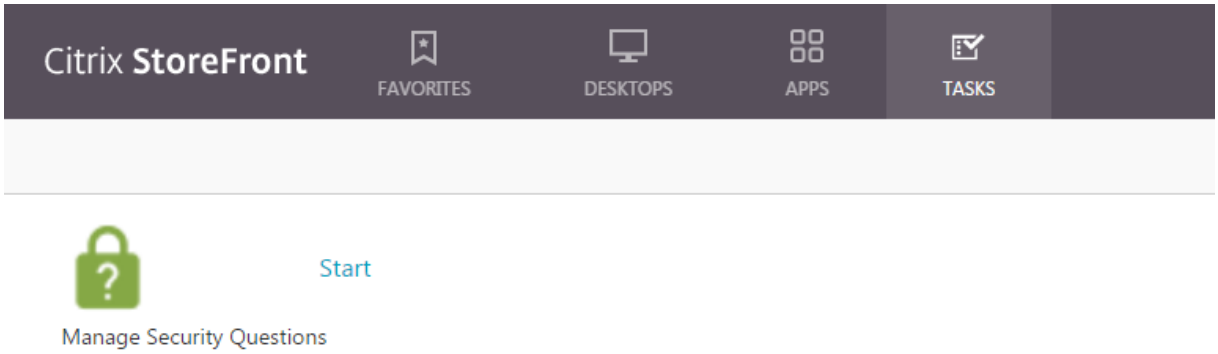
1. Para que se pueda usar el Autoservicio de restablecimiento de contraseñas en StoreFront, seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar métodos de autenticación > Nombre de usuario 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.



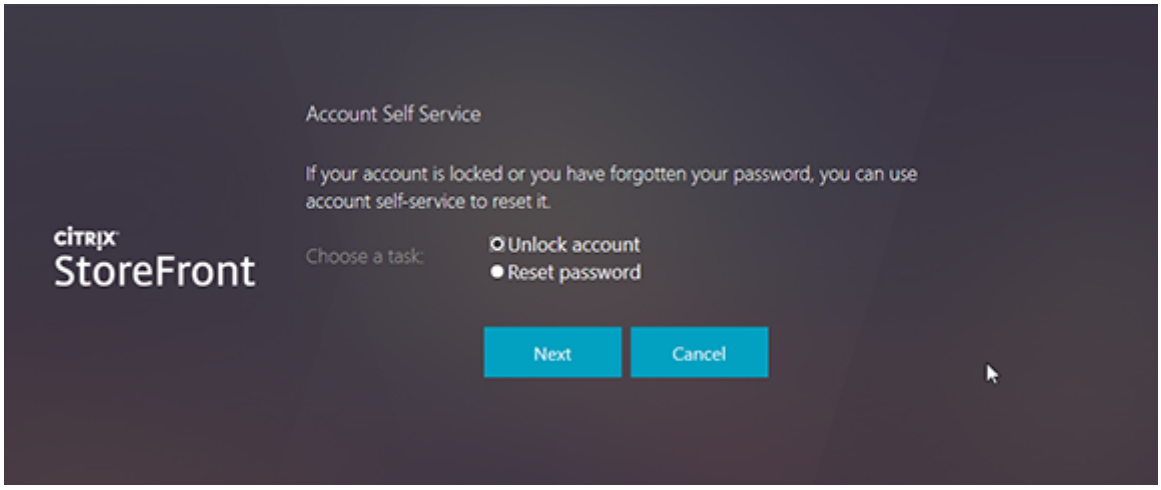
La próxima vez que el usuario inicie sesión en la aplicación Citrix Workspace o Citrix Receiver para Web, la inscripción de seguridad estará disponible. Después de hacer clic en **Iniciar**, el usuario verá preguntas a las que tiene que responder.



Una vez configurados en StoreFront, los usuarios ven el enlace **Autoservicio de cuentas** en la pantalla de inicio de sesión de Citrix Receiver para Web (se muestra como un botón en otras aplicaciones Citrix Workspace).

Al hacer clic en este enlace, el usuario pasa por una serie de formularios para seleccionar 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 `username@domain.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 Shared Authentication Service Settings para especificar los almacenes que compartirán el servicio de autenticación al habilitar el inicio sesión Single Sign-On.

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. 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 un almacén en el menú desplegable **Almacén**.

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

Delegar la validación de credenciales a Citrix Gateway

Si quiere habilitar la autenticación PassThrough para los usuarios de tarjeta inteligente que acceden a los almacenes a través de Citrix Gateway, use la tarea Configurar autenticación delegada. Esta tarea solo está disponible cuando la opción “PassThrough desde Citrix Gateway” está habilitada y seleccionada en el panel de resultados.

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

Autenticación basada en el servicio XML

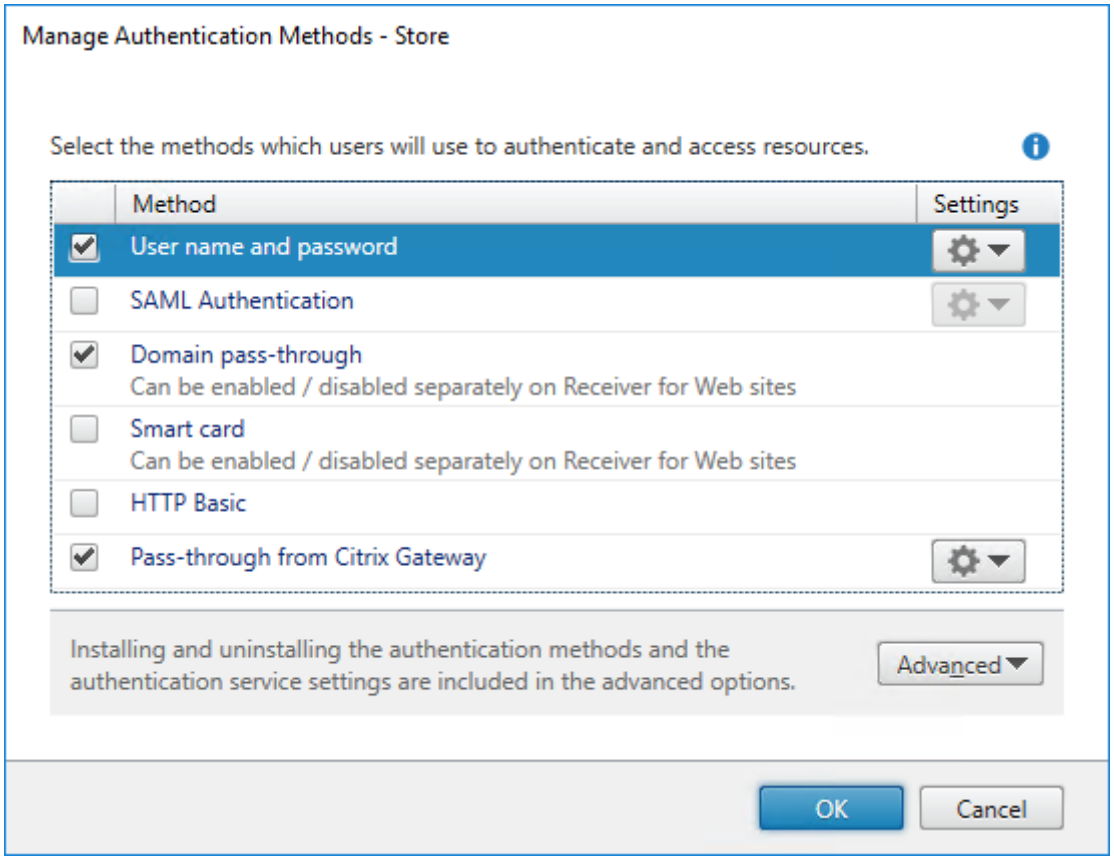
August 22, 2019

Si StoreFront no está en el mismo dominio que Citrix Virtual Apps and Desktops, y no se pueden establecer relaciones de confianza de Active Directory, puede configurar StoreFront para que use el ser-

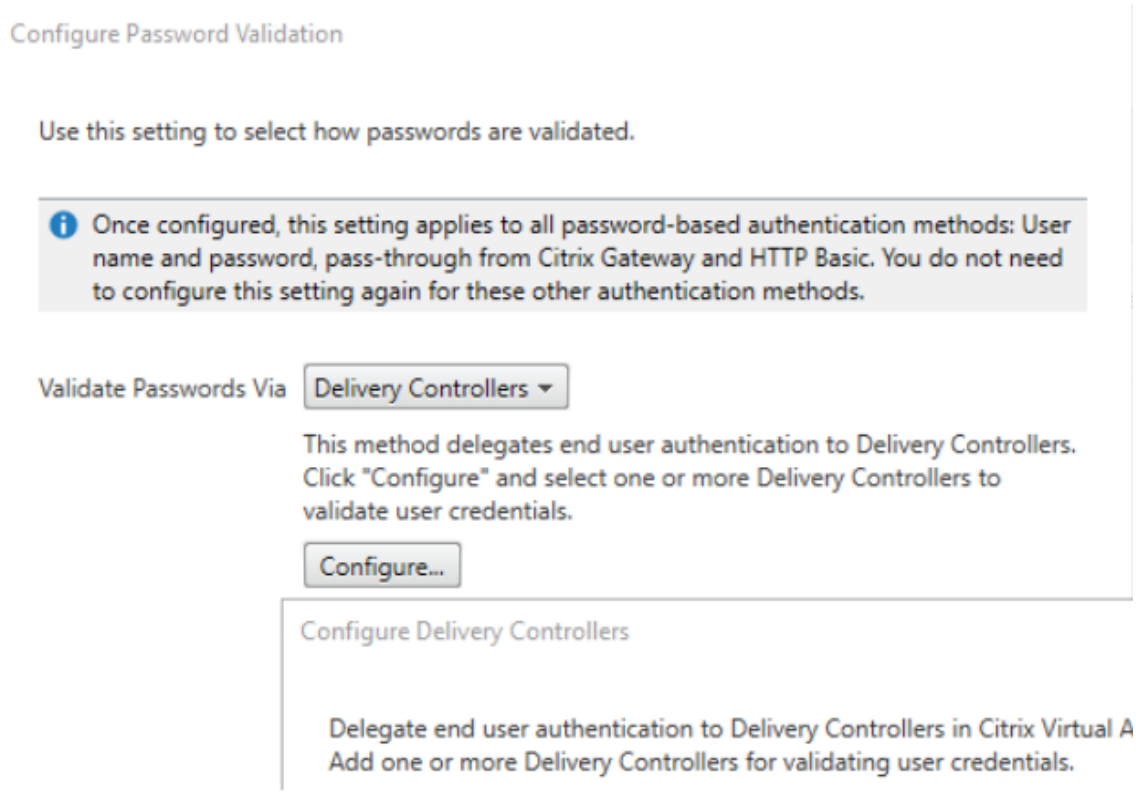
vicio XML de Citrix Virtual Apps and Desktops en la autenticación de las credenciales de nombre de usuario y contraseña.

Habilitar la autenticación basada en el servicio XML

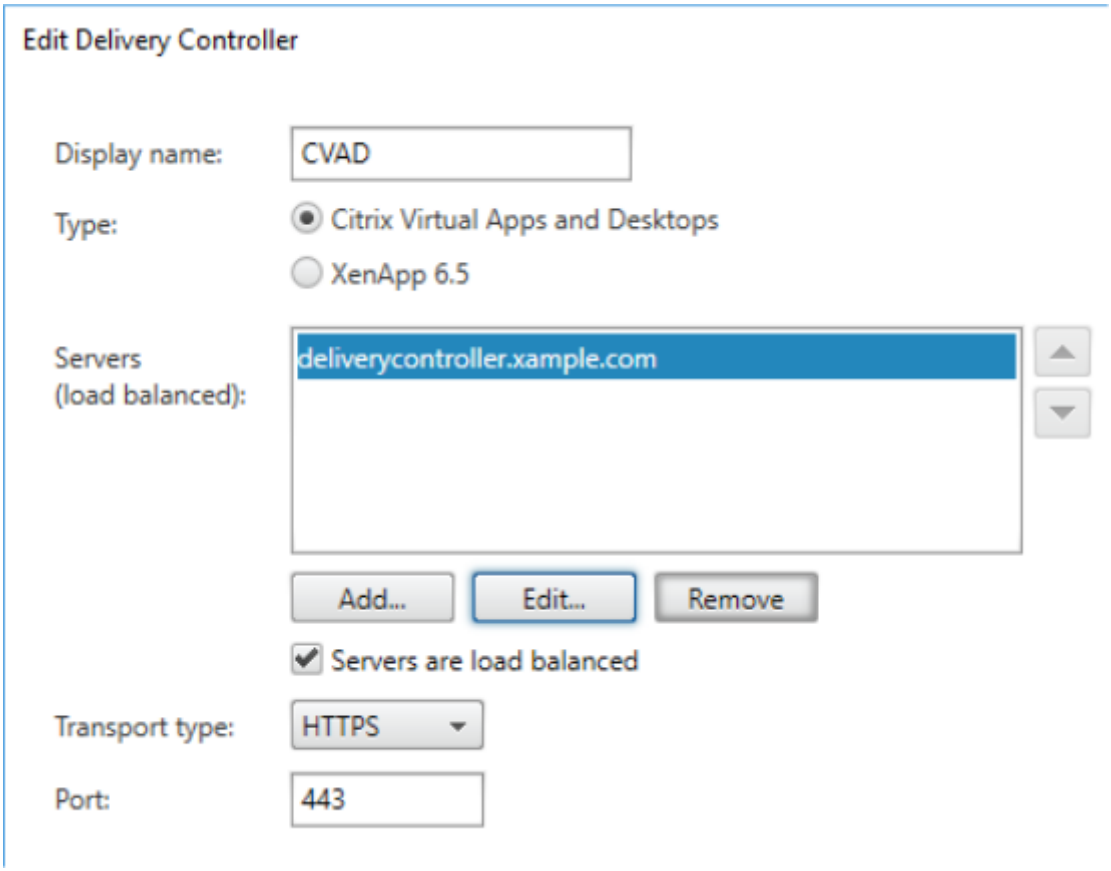
1. En la pantalla de **Inicio** o **Aplicaciones** de Windows, busque el icono de Citrix StoreFront y haga clic en él.
2. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar métodos de autenticación**.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



4. En la lista **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 **Almacenes** 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**.

Configurar la delegación Kerberos limitada para XenApp 6.5

January 6, 2020

> Nota:
>
> XenApp 6.5 ha alcanzado el ciclo Fin de vida (EOL) y ahora lo cubre el programa de soporte extendido Extended Support Program.

Utilice la tarea **Configurar parámetros del almacén** > **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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás 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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel Acciones, haga clic en **Configurar parámetros del almacén** y, a continuación, haga clic en Delegación Kerberos.
3. Habilite o inhabilite la delegación de Kerberos para autenticarse en los Delivery Controllers.

Configurar el servidor de StoreFront para la delegación

Siga este procedimiento cuando StoreFront no esté instalado en la misma máquina que Citrix Virtual Apps.

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 de StoreFront.
4. En el panel **Acciones**, haga clic en **Propiedades**.
5. En la ficha **Delegación**, haga clic en **Confiar en este equipo para la delegación solo 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 XML Service de Citrix Virtual Apps and Desktops 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.

Configurar el servidor Citrix Virtual Apps para la delegación

Configure la delegación de confianza de Active Directory para cada servidor Citrix Virtual Apps.

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 XML Service de Citrix Virtual Apps and Desktops al que StoreFront está configurado para conectarse.
3. En el panel **Acciones**, haga clic en **Propiedades**.
4. En la ficha **Delegación**, haga clic en **Confiar en este equipo para la delegación solo 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 XML Service de Citrix Virtual Apps and Desktops 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 **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 quiere seleccionar** y, a continuación, haga clic en **Aceptar**.
9. Seleccione los tipos de servicio **cifs** e **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 elegir el nombre de usuario local y la contraseña en la plantilla icaclient.adm de Citrix que quiera (controla la función 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 configu-

ración 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 de 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 elegir el nombre de usuario local y la contraseña en la plantilla icaclient.adm de Citrix que quiera (controla la función ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - Habilite el método de autenticación con tarjeta inteligente en el servidor de 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.
- Citrix 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 elegir el nombre de usuario local y la contraseña en la plantilla icaclient.adm de Citrix que quiera (controla la función ssonsvr.exe).
  - El parámetro Kerberos de la plantilla icaclient.adm es obligatorio.
  - Habilite el método de autenticación PassThrough desde Citrix Gateway en el servidor de 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 Citrix 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 Citrix Gateway.
- Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows (AuthManager), autenticación con tarjeta inteligente con solicitud de PIN y StoreFront:
  - No necesita ssonsvr.exe en el cliente.
  - Puede elegir el nombre de usuario local y la contraseña en la plantilla icaclient.adm de Citrix que quiera (controla la función 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 de StoreFront.
- Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows (AuthManager), Kerberos y StoreFront:
  - No necesita ssonsvr.exe en el cliente.
  - Puede elegir el nombre de usuario local y la contraseña en la plantilla icaclient.adm de Citrix que quiera (controla la función 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 de StoreFront.
  - Compruebe que se ha definido esta clave de Registro:

    > **Precaución:**
    > Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar 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. Haga una copia de seguridad del Registro antes de modificarlo.

    Para máquinas de 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integrate
    Nombre: SSONCheckEnabled
    Tipo: REG_SZ
    Valor: true o false
    Para máquinas de 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerPro
    Nombre: SSONCheckEnabled
    Tipo: REG_SZ
    Valor: true o false

Configurar la autenticación con tarjeta inteligente

January 6, 2020

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.

El documento Configuración de tarjetas inteligentes para entornos Citrix describe cómo configurar un entorno de Citrix para tarjetas inteligentes con un tipo de tarjeta inteligente específico. Para tarjetas inteligentes de otros proveedores hay que seguir un proceso similar.

> Nota:
>
> En este artículo, las menciones de “aplicación Citrix Workspace” también representan las versiones compatibles de Citrix Receiver, a menos que se indique lo contrario.

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 de StoreFront, o bien, dentro de un dominio que tenga una relación de confianza bidireccional directa con el dominio del servidor de 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 Citrix Virtual Desktops, 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.

Configurar Citrix Gateway

- En el dispositivo Citrix Gateway, instale un certificado de servidor firmado por una entidad de certificación. Para obtener más información, consulte Instalar y administrar certificados.
- En el dispositivo Citrix Gateway, instale 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 Citrix 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 Configuring and Binding a Client Certificate Authentication Policy.
- 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 Configurar la autenticación con tarjeta inteligente.

  También debe configurar StoreFront para redirigir 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. Tras establecerse la conexión, los usuarios ya no necesitan autenticarse en Citrix Gateway, pero tienen que introducir sus PIN para iniciar 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 perfiles y directivas de sesión para conexiones de Citrix Gateway a StoreFront y enlácelos al servidor virtual correspondiente. Para obtener más información, consulte Acceder a StoreFront a través de Citrix 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. Solo StoreFront utiliza este servidor virtual para comprobar las solicitudes del dispositivo Citrix Gateway y, por lo tanto, no es necesario que se pueda acceder públicamente a él. 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 Creación de servidores virtuales.

Configurar 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 sobre cómo crear un certificado de servidor en IIS, consulte https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard. Para obtener más información acerca de cómo agregar un enlace HTTPS a un sitio IIS, consulte https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11).

- Si quiere exigir que se presenten certificados del cliente para las conexiones HTTPS con todas las direcciones URL de StoreFront, configure IIS en el servidor de 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 a todas las direcciones URL de StoreFront, los usuarios de tarjetas inteligentes no pueden conectarse a través de Citrix 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 los almacenes deben colocarse en el mismo servidor y debe utilizarse un certificado del cliente válido para todos los almacenes. 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.

- Instale y configure StoreFront. Cree el servicio de autenticación y agregue los almacenes que necesite. Si configura el acceso remoto a través de Citrix Gateway, no habilite la integración de VPN. Para obtener más información, consulte Instalar y configurar 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 almacenes a través de Citrix Gateway, habilite el método de autenticación PassThrough con Citrix Gateway y compruebe que StoreFront está configurado para delegar la validación de credenciales a Citrix Gateway. Si va a habilitar la autenticación PassThrough al instalar Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows en dispositivos de usuario unidos a un dominio, habilite la autenticación PassThrough de dominio. Para obtener más información, consulte Configurar el 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 Configurar sitios de Citrix Receiver para web.

  Si quiere 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 quiere habilitar la autenticación PassThrough al instalar Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows en los dispositivos de usuario unidos a un dominio, modifique el archivo default.ica del almacén en el que quiere habilitar la autenticación PassThrough

de credenciales con tarjeta inteligente de los usuarios cuando acceden a sus escritorios y aplicaciones. Para obtener más información, consulte Habilitar la autenticación PassThrough con tarjeta inteligente en Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows.

- Si ha creado un servidor virtual de Citrix Gateway adicional para utilizarlo únicamente en las conexiones de usuario a los recursos, configure el enrutamiento óptimo de Citrix Gateway a través de este servidor virtual para las conexiones a las implementaciones que proporcionan los escritorios y las aplicaciones del almacén. Para obtener más información, consulte Configurar el enrutamiento HDX óptimo para un almacén.
- Para permitir que los usuarios de dispositivos de escritorio con Citrix Desktop Lock puedan autenticarse con tarjetas inteligentes, habilite la autenticación PassThrough con tarjeta inteligente para las direcciones URL de XenApp Services. Para obtener más información, consulte Configuración de la autenticación de las direcciones URL de XenApp Services.

Configurar 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 reasignados, instale Receiver para Windows (Enterprise) mediante una cuenta con permisos de administrador. Configure Receiver para Windows con la URL de XenApp Services para el almacén correspondiente. Una vez que haya confirmado que puede iniciar sesión en el dispositivo con una tarjeta inteligente y acceder a los recursos del almacén, instale Citrix Desktop Lock. Para obtener más información, consulte Para instalar Desktop Lock.
- Para todos los demás usuarios, instale la versión de la aplicación Citrix Workspace pertinente en el dispositivo de usuario. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente en Citrix Virtual Apps and Desktops cuando se trate de usuarios con dispositivos unidos a un dominio, use una cuenta con permisos de administrador para instalar la aplicación Citrix Workspace para Windows en una ventana del símbolo del sistema con la opción **/includeSSON**. Para obtener más información, consulte Usar parámetros de línea de comandos.

  Asegúrese de que la aplicación Citrix Workspace para Windows está configurado para la autenticación con tarjeta inteligente a través de una directiva de dominio o una directiva de equipo local. Para crear una directiva de dominio, use la Consola de administración de directivas de grupo para importar el archivo de plantilla del objeto de directiva de grupo de la aplicación Citrix Workspace para Windows, icaclient.adm, en el controlador de dominio para el dominio que contiene las cuentas de sus 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 Tarjeta inteligente.

Habilite la directiva Autenticación con tarjeta inteligente. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente de los usuarios, seleccione Usar autenticación PassThrough para el PIN. A continuación, para la autenticación PassThrough de las credenciales con tarjeta inteligente de los usuarios a través de Citrix Virtual Apps and Desktops, habilite la directiva Nombre de usuario y contraseña locales y seleccione Permitir autenticación PassThrough para todas las conexiones ICA. Para obtener más información, consulte Referencia para parámetros ICA.

Si ha habilitado la autenticación PassThrough de credenciales con tarjeta inteligente en Citrix Virtual Apps and Desktops para los usuarios con dispositivos unidos a un dominio, agregue la URL del almacén a la zona de Intranet local o Sitios de confianza de Internet Explorer. Asegúrese de que el inicio de sesión automático con el nombre de usuario y la contraseña actuales esté seleccionado en los parámetros de seguridad de la zona.

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

Habilitar la autenticación PassThrough con tarjeta inteligente en Citrix Receiver para Windows o la aplicación Citrix Workspace 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 Citrix Virtual Apps and Desktops, modifique el archivo default.ica del almacén.

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

1. Utilice un editor de texto para abrir el archivo default.ica del almacén. Por regla general, este archivo se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storename\App_Data\, donde storename es el nombre especificado para el almacén durante su creación.
2. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente para usuarios que acceden a almacenes sin Citrix Gateway, agregue el siguiente parámetro a la sección [Aplicación].


```
DisableCtrlAltDel=Off
```

Este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar tanto la autenticación PassThrough de dominio como la autenticación PassThrough con tarjeta inteligente para acceder a los escritorios y las aplicaciones, debe crear almacenes independientes para cada método de autenticación. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.

3. Para habilitar la autenticación PassThrough de credenciales con tarjeta inteligente para usuarios que acceden a almacenes a través de Citrix Gateway, agregue el siguiente parámetro a la sección [Aplicación].

```
UseLocalUserAndPassword=On
```

Este parámetro se aplica a todos los usuarios del almacén. Si quiere habilitar la autenticación PassThrough para algunos usuarios y requerir que otros inicien sesión para acceder a sus escritorios y aplicaciones, debe crear almacenes independientes para cada grupo de usuarios. A continuación, debe dirigir a los usuarios al almacén adecuado para su método de autenticación.

Configurar el período de notificación sobre caducidad de contraseñas

June 24, 2019

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, modifique 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado, propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

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 **Almacenes** 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.

Configurar y administrar almacenes

January 6, 2020

En Citrix StoreFront, puede crear y administrar almacenes que combinan escritorios y aplicaciones desde Citrix Virtual Apps and Desktops, con lo que ofrecerá a los usuarios un acceso de autoservicio y a demanda a los recursos.

Tarea	Detalles
Crear o quitar un almacén	Configura tantos almacenes adicionales como se necesiten.
Crear un almacén no autenticado	Configura más almacenes no autenticados para permitir el acceso de usuarios no autenticados (anónimos).
Exportar archivos de aprovisionamiento de almacenes para los usuarios	Genera archivos que contengan datos de conexión a los almacenes, incluidas las implementaciones de Citrix Gateway y las balizas configuradas para los almacenes.
Formas de ocultar y publicar almacenes para los usuarios	Evita que se muestren los almacenes a los usuarios y, por tanto, que los puedan agregar a sus cuentas cuando configuren la aplicación Citrix Workspace mediante la detección de cuentas basada en direcciones de correo electrónico o FQDN.
Administrar los recursos disponibles en los almacenes	Agrega y quita recursos de los almacenes.
Administrar el acceso remoto a los almacenes a través de Citrix Gateway	Configura el acceso a los almacenes a través de Citrix Gateway para los usuarios que se conectan desde redes públicas.

Tarea	Detalles
Configurar dos almacenes de StoreFront para compartir un almacén de datos de suscripción común	Configura dos almacenes para que compartan una base de datos de suscripción común.
Parámetros avanzados de los almacenes	Configura los parámetros avanzados de los almacenes.

Crear o quitar un almacén

March 2, 2020

Utilice la tarea **Crear almacén** para configurar almacenes adicionales. Puede crear tantos almacenes como necesite. Por ejemplo: puede crear un almacén para un determinado grupo de usuarios o para agrupar un conjunto específico de recursos.

Para crear un almacén, identifique y configure las comunicaciones con los servidores que ofrecen los recursos que quiere entregar desde ese almacén. A continuación, opcionalmente, configure el acceso remoto al almacén a través de Citrix Gateway.

En la página Nombre de almacén, al seleccionar **Permitir el acceso a este almacén solo a usuarios no autenticados** le permite crear un almacén no autenticado, que es anónimo o no autenticado. Cuando se crea un almacén no autenticado, las páginas **Métodos de autenticación** y **Acceso remoto** no están disponibles, mientras que **Nodo de grupo de servidores** situado a la izquierda y el panel Acciones se reemplazan por **Cambiar URL base**. (Esta es la única opción disponible porque los grupos de servidores no están disponibles en servidores que no están unidos a un dominio).

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

Agregar escritorios y aplicaciones al almacén

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Crear almacén**.
3. En la página **Nombre del almacén**, especifique un nombre para el almacén y haga clic en **Siguiente**.

   Los nombres de los almacenes aparecen en la aplicación Citrix Workspace, en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido de cada almacén.
4. En la página **Delivery Controllers**, indique la infraestructura que ofrece los recursos que estarán disponibles en el almacén. Haga clic en **Agregar**.
5. En el cuadro de diálogo Agregar Delivery Controller, especifique un **nombre simplificado** que le ayude a identificar la implementación. Especifique **Tipo** para indicar cómo se ofrecen los recursos disponibles en el almacén. Escriba los valores predeterminados para Citrix Virtual Apps and Desktops. Puede seleccionar XenApp 6.5 como Tipo, pero este producto ha alcanzado el ciclo Fin de vida (EOL) en junio de 2018 y ahora lo cubre el programa de soporte extendido Extended Support Program.
6. Para que los escritorios y las aplicaciones que ofrece Citrix Virtual Apps and Desktops y XenApp 6.5 estén disponibles en el almacén, agregue los nombres o las direcciones IP de sus servidores a la lista **Servidores**. Puede indicar varios servidores si quiere ofrecer una tolerancia a fallos. Para ello, especifique las entradas por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para los sitios de Citrix Virtual Apps and Desktops, proporcione datos de los Delivery Controllers. En el caso de las comunidades de XenApp 6.5, indique los servidores con Citrix XML Service.
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 TLS (Transport Layer Security), seleccione **HTTPS**. Si selecciona esta opción para servidores Citrix Virtual Apps and Desktops, debe comprobar 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 6.5 mediante 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 servidores Citrix Virtual Apps and Desktops, el puerto especificado debe ser el puerto que Citrix XML Service utilice.
9. Si utiliza el Traspaso SSL para proteger las conexiones entre StoreFront y los servidores de XenApp 6.5, 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 almacenes para proporcionar recursos desde cualquier combinación de implementaciones de Citrix Virtual Apps and Desktops. Repita todos los pasos del 4 al 10, según sea necesario, para indicar implementaciones adicionales que proporcionen recursos para el almacén. Una vez que haya agregado todos los recursos necesarios para el almacén, haga clic en **Siguiente**.
11. En la página **Acceso remoto**, especifique si los usuarios que se conectan desde redes públicas pueden acceder al almacén a través de Citrix Gateway y la forma en que pueden hacerlo.
    - Para que el almacén no esté disponible para los usuarios de redes públicas, deje sin marcar la casilla **Habilitar acceso remoto**. Solo los usuarios locales de la red interna podrán acceder al almacén.
    - Para habilitar el acceso remoto, seleccione **Habilitar acceso remoto**.
      - Para que solo los recursos entregados mediante Citrix Gateway estén disponibles en el almacén, seleccione **Sin túnel VPN**. Los usuarios inician sesión en Citrix Gateway con ICAproxy o una VPN sin cliente (cVPN), y no necesitan usar el plug-in de Citrix Gateway para establecer una VPN completa.
      - Para determinar que el almacén y todos los demás recursos de la red interna estén disponibles a través de un túnel de red privada virtual (VPN) con capa de sockets seguros (SSL), seleccione **Túnel VPN completo**. Los usuarios necesitan el plug-in de Citrix Gateway para establecer el túnel VPN.

    Al habilitar el acceso remoto al almacén, el método de autenticación **PassThrough desde Citrix Gateway** se habilita automáticamente. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes.

12. Si ha habilitado el acceso remoto, en la lista **Dispositivos Citrix Gateway**, seleccione los dispositivos (implementaciones) a través de los cuales los usuarios pueden acceder al almacén. Las implementaciones previamente configuradas para este y otros almacenes están disponibles y se pueden seleccionar de la lista. Si habilita el acceso a través de varios dispositivos porque selecciona más de una entrada de la lista, especifique el **Dispositivo predeterminado** que se utilizará para acceder al almacén. Para agregar más dispositivos a la lista, siga el proceso descrito en Ofrecer acceso remoto al almacén a través de Citrix Gateway.
13. En la página **Configurar métodos de autenticación**, seleccione los métodos que utilizarán los usuarios para autenticarse y acceder al almacén, 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 los almacenes.
    - **Autenticación SAML:** Los usuarios se autentican en un proveedor de identidades y su sesión se inicia automáticamente cuando acceden a sus almacenes.
    - **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 los almacenes.
    - **Tarjeta inteligente:** Los usuarios se autentican con tarjetas inteligentes y números PIN cuando acceden a los almacenes.
    - **HTTP básica:** Los usuarios se autentican en el servidor web IIS del servidor de StoreFront.
    - **PassThrough desde Citrix Gateway:** Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes. Esta opción se selecciona automáticamente cuando se habilita el acceso remoto. En la página **Configurar validación de contraseñas**, seleccione los Delivery Controllers que ofrecen la validación de contraseñas y haga clic en **Siguiente**.
14. En la página **URL de XenApp Services**, defina la URL para los usuarios que usen PNAgent para acceder a las aplicaciones y los escritorios. A continuación, haga clic en **Crear**.
15. Después de haber creado el almacén, haga clic en **Finalizar**.

Acceder al almacén

Ahora, el almacén está disponible para que los usuarios accedan a él mediante la aplicación Citrix Workspace, que debe estar configurada con los datos de acceso al almacén. Existen diversas maneras de proporcionar esta información a los usuarios y facilitarles el proceso de configuración. Para obtener más información, consulte Opciones de acceso de los usuarios.

De manera alternativa, los usuarios pueden acceder al almacén 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 al nuevo almacén, aparece al crearlo.

Al crear un almacén, la URL de XenApp Services correspondiente se habilita de forma predeterminada. Los usuarios de dispositivos de escritorio con Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a los almacenes directamente mediante la URL de XenApp Services de cada almacén. La dirección URL de XenApp Services 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 el almacén en el paso 3.

Ofrecer acceso remoto al almacén a través de Citrix Gateway

Complete los siguientes pasos para configurar el acceso remoto, a través de Citrix Gateway, al almacén que ha creado en el procedimiento anterior. Se presupone que ha completado todos los pasos anteriores.

1. En la página **Acceso remoto** del **asistente para crear almacenes**, haga clic en **Agregar**.
2. En el cuadro de diálogo **Agregar dispositivo Citrix Gateway**, en la página **Parámetros generales**, especifique un **nombre simplificado** para el dispositivo Citrix Gateway que ayudará a los usuarios a identificarlo.

   Los usuarios verán el nombre simplificado que especifique en la aplicación Citrix Workspace, de modo que debe incluir la información relevante en el nombre para ayudarlos a decidir si utilizar esa puerta de enlace o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de Citrix Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.
3. En **URL de Citrix Gateway**, escriba la combinación URL:puerto del servidor virtual de Citrix Gateway de la implementación. Si no especifica ningún puerto, se utiliza el puerto predeterminado `https://` de 443. No es necesario especificar el puerto 443 en la URL.

   El nombre de dominio completo (FQDN) de la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de Citrix Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de Citrix Gateway.
4. Seleccione el **Uso o rol** de Citrix Gateway a partir de las opciones disponibles.
   - **Autenticación y enrutamiento de HDX:** Citrix Gateway se usará para la autenticación y para el enrutamiento de las sesiones HDX.
   - **Solo autenticación:** Citrix Gateway se usará para la autenticación, no para el enrutamiento de las sesiones HDX.

- **Solo enrutamiento de HDX:** Citrix Gateway se usará para enrutar sesiones HDX, no para la autenticación.

5. Para todas aquellas implementaciones en las que los recursos que ofrezcan Citrix Virtual Apps and Desktops o XenApp 6.5 estarán disponibles en el almacén, indique las direcciones URL de Secure Ticket Authority (STA) de los servidores que ejecutan STA en la página **Secure Ticket Authority**. 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 Citrix Virtual Apps and Desktops o XenApp 6.5. Emite tíquets de sesión en respuesta a las solicitudes de conexión. Esos tíquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de Citrix Virtual Apps and Desktops o XenApp 6.5. Utilice la URL de STA correcta (como `HTTPS://` o `HTTP://`), según cómo estén configurados los Delivery Controllers. La dirección URL de STA también debe ser idéntica a la configurada en el dispositivo Citrix Gateway presente en el servidor virtual.

6. Elija el 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. Para garantizar que Citrix Virtual Apps and Desktops o XenApp 6.5 mantengan abiertas las sesiones desconectadas mientras la aplicación Citrix Workspace intenta volver a conectarse automáticamente, seleccione **Habilitar fiabilidad de la sesión**.

8. Si ha configurado varios STA y quiere que la fiabilidad de la sesión esté siempre disponible, seleccione **Solicitar tíquets de dos STA, si están disponibles**. StoreFront obtiene tíquets de sesión de dos STA diferentes, con lo que las sesiones de usuario no se interrumpen si un STA deja de estar disponible durante la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.

9. En la página **Parámetros de autenticación**, escriba la **dirección IP del servidor virtual** (VIP) que tenga el dispositivo Citrix Gateway.

   Utilice la dirección IP privada para el servidor virtual de Citrix Gateway, en lugar de la dirección IP pública que está vinculada por NAT a la dirección IP privada. StoreFront suele identificar las puertas de enlace a través de sus URL. Si está utilizando GSLB (equilibrio de carga del servidor global), debe agregar la dirección IP virtual a cada puerta de enlace. Eso permite a StoreFront identificar varias puertas de enlace que utilizan la misma URL (nombre de dominio GSLB) como puertas de enlace distintas. Por ejemplo, el almacén puede tener configuradas tres puertas de enlace con la misma URL, como `https://gslb.domain.com`, pero cada una tendría direcciones IP virtuales únicas configuradas como 10.0.0.1, 10.0.0.2 y 10.0.0.3.

10. Si quiere agregar un dispositivo con Citrix Gateway, seleccione en la lista **Tipo de inicio de sesión** el método de autenticación configurado en el dispositivo para los usuarios de la aplicación Citrix Workspace.

- 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. Si está configurando StoreFront para Citrix Gateway y quiere usar SmartAccess, debe escribir una **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 Citrix Gateway para verificar que las solicitudes recibidas desde Citrix Gateway provienen de ese dispositivo.

    Cuando se utilice GSLB, se recomienda que configure direcciones URL de respuesta únicas para cada una de las puertas de enlace de GSLB. StoreFront debe poder resolver cada una de las URL de respuesta únicas y recurrir a las direcciones IP virtuales privadas configuradas para cada uno de los servidores virtuales de puerta de enlace de GSLB. Por ejemplo, `emeagateway.domain.com`, `usgateway.domain.com` y `apacgateway.domain.com` deben recurrir a la dirección IP virtual de la puerta de enlace correcta.

12. Haga clic en **Crear** para agregar su dispositivo Citrix Gateway a la lista del cuadro de diálogo **Configurar parámetros de acceso remoto**.

    La información sobre la configuración de los dispositivos Citrix Gateway se guarda en el archivo de aprovisionamiento .cr del almacén. Eso permite que la aplicación Citrix Workspace envíe la solicitud de conexión pertinente al comunicarse con los dispositivos por primera vez.

Quitar un almacén

Utilice la tarea Quitar almacén para eliminar un almacén. Al eliminar un almacén, también se eliminan los sitios asociados de Receiver para Web y las direcciones URL de XenApp Services.

> **Importante:**
>
> En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en

> la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado, propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

Crear un almacén no autenticado

March 2, 2020

Utilice la tarea Crear almacén para usuarios no autenticados si quiere configurar más almacenes no autenticados y así admitir el acceso de usuarios no autenticados (anónimos). Puede crear tantos almacenes no autenticados como necesite. Por ejemplo: puede crear un almacén no autenticado para un determinado grupo de usuarios o para agrupar un conjunto específico de recursos.

El acceso remoto mediante Citrix Gateway no se puede aplicar a almacenes no autenticados.

Para crear un almacén no autenticado, identifique y configure las comunicaciones con los servidores que proporcionan los recursos que quiere poner en el almacén.

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

Agregar escritorios y aplicaciones al almacén

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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Crear almacén**.
3. En la página “Nombre del almacén”, especifique un nombre para el almacén, seleccione **Permitir el acceso a este almacén solo a usuarios no autenticados (anónimos)** y haga clic en **Siguiente**.

   Los nombres de los almacenes aparecen en Citrix Receiver en las cuentas de los usuarios. Por esa razón, elija nombres que informen a los usuarios sobre el contenido del almacén.

4. En la página **Delivery Controllers**, indique la infraestructura que ofrece los recursos que estarán disponibles en el almacén. 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 Citrix Virtual Apps and Desktops o XenApp 6.5 ofrece los recursos que quiere poner a disposición en el almacén. (Nota: XenApp 6.5 ha alcanzado el fin de ciclo de vida (EOL) y ahora está cubierto por el programa Extended Support Program.) Al asignar Delivery Controllers, asegúrese de que solo utiliza aquellos que admiten la función de aplicaciones anónimas. Si configura su almacén no autenticado con Controllers que no admiten esta función, es posible que no haya ninguna aplicación anónima disponible en el almacén.

   Para que los escritorios y las aplicaciones que ofrecen las comunidades de XenApp 6.5 estén disponibles en el almacén, agregue el nombre de todos los servidores de la comunidad a la lista Servidores. Puede indicar varios servidores si quiere ofrecer una tolerancia a fallos. Para ello, especifique las entradas por orden de prioridad con el objetivo de definir la secuencia de conmutación por error. Para los sitios de Citrix Virtual Desktops, proporcione datos de los Controllers. En el caso de las comunidades de XenApp 6.5, indique los servidores con Citrix XML Service.

6. 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 Citrix Virtual Apps and Desktops, debe comprobar 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.

7. 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 servidores Citrix Virtual Apps and Desktops, el puerto especificado debe ser el puerto que Citrix XML Service utilice.

8. Haga clic en **Aceptar**. Puede configurar almacenes para proporcionar recursos desde cualquier

combinación de implementaciones de Citrix Virtual Apps and Desktops. Repita todos los pasos del 4 al 9, según sea necesario, para indicar implementaciones adicionales que proporcionen recursos para el almacén. Una vez que haya agregado todos los recursos necesarios para el almacén, haga clic en **Crear**.

Ahora ya podrá utilizar el almacén no autenticado. Para habilitar el acceso de usuarios al nuevo almacén, la aplicación Citrix Workspace debe configurarse con la información de acceso del almacén. Existen diversas maneras de proporcionar esta información a los usuarios y facilitarles el proceso de configuración. Para obtener más información, consulte
Opciones de acceso de los usuarios.

Los usuarios también pueden acceder al almacén 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 almacenes no autenticados, 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 al nuevo almacén, aparece al crearlo.

Al crear un almacén, la URL de XenApp Services correspondiente se habilita de forma predeterminada. Los usuarios de dispositivos de escritorio unidos a un dominio y los equipos reasignados con Citrix Desktop Lock, junto con usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a los almacenes directamente mediante la URL de XenApp Services de cada almacén. La dirección URL de XenApp Services 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 el almacén 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 Citrix Receiver para Web que acceden a este almacén no autenticado no finalizarán. Normalmente, el archivo web.config se encuentra en `C:\inetpub\wwwroot\Citrix\storename\`, donde **storename** es el nombre especificado para el almacén cuando este se creó. Para que estas sesiones finalicen correctamente, el servidor XenApp que utilice este almacén 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.

Exportar archivos de aprovisionamiento de almacenes para los usuarios

March 2, 2020

Utilice las tareas **Exportar archivo de aprovisionamiento multialmacén** y **Exportar archivo de aprovisionamiento** para generar archivos que contengan datos de conexión para los almacenes, incluidas las implementaciones de Citrix Gateway y las balizas configuradas para los almacenes. Ponga estos archivos a disposición de los usuarios para permitirles que configuren la aplicación Citrix Workspace automáticamente con la información de los almacenes. Los usuarios también pueden obtener los archivos de aprovisionamiento de la aplicación Citrix Workspace 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado,
> propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

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

Anunciar y ocultar almacenes para los usuarios

July 25, 2019

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

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

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Configurar parámetros del almacén** > **Anunciar almacén**.
3. En la página **Anunciar almacén**, seleccione **Anunciar almacén** u **Ocultar almacén**.

Administrar los recursos disponibles en los almacenes

March 2, 2020

Utilice la tarea **Administrar Delivery Controllers** para agregar o quitar los recursos que proporciona Citrix Virtual Apps and Desktops dentro de un almacén, 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado,
> propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel Acciones, haga clic en **Administrar Delivery Controllers**.
3. En el cuadro de diálogo “Administrar Delivery Controllers”:
    a) Haga clic en **Agregar** para incluir en el almacén escritorios y aplicaciones de otra implementación de Citrix Virtual Apps and Desktops.

b) Haga clic en **Modificar** para cambiar los parámetros de una implementación.
c) Seleccione una entrada de la lista de Delivery Controllers y haga clic en **Quitar** para detener los recursos proporcionados por la implementación que está disponible en el almacén.

4. En el cuadro de diálogo Agregar Controller o Modificar Controller, especifique un **nombre simplificado** que le ayude a identificar la implementación.
5. Para que los escritorios y las aplicaciones que proporciona Citrix Virtual Apps and Desktops estén disponibles en el almacén, 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 Citrix Virtual Desktops, proporcione datos de los Delivery Controllers. En el caso de las comunidades de Citrix Virtual Apps, enumere los servidores que ejecutan Citrix XML Service. Para modificar el nombre o la dirección IP de un servidor, seleccione la entrada correspondiente en 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.
6. 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 Citrix Virtual Apps and Desktops, debe comprobar 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 Citrix Virtual Apps 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.

7. 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 servidores Citrix Virtual Apps and Desktops, el puerto especificado debe ser el puerto que Citrix XML Service utilice.

8. Si utiliza el Traspaso SSL para proteger las conexiones entre los servidores Citrix Virtual Apps y StoreFront, 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.
9. Haga clic en **Aceptar**. Puede configurar almacenes para proporcionar recursos desde cualquier combinación de implementaciones de Citrix Virtual Apps and Desktops. Repita los pasos del 3 al 9, tantas veces como sea necesario, para agregar o modificar otras implementaciones de la lista de Delivery Controllers.

Administrar el acceso remoto a los almacenes a través de Citrix Gateway

January 6, 2020

Utilice la tarea Configurar parámetros de acceso remoto para definir el acceso a los almacenes a través de Citrix Gateway que se les otorga a los usuarios que se conectan desde redes públicas. El acceso remoto mediante Citrix Gateway no se puede aplicar a almacenes no autenticados.

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

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 Almacenes en el panel derecho de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. 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 al almacén a través de Citrix Gateway y la forma en que pueden hacerlo.
    - Para que el almacén no esté disponible para los usuarios de redes públicas, deje sin marcar la casilla **Habilitar acceso remoto**. Solo los usuarios locales de la red interna podrán acceder al almacén.

- Para habilitar el acceso remoto, marque la casilla **Habilitar acceso remoto**.
  - Para que los recursos entregados mediante Citrix Gateway estén disponibles en el almacén, seleccione **Sin túnel VPN**. Los usuarios inician sesión en Citrix Gateway con ICAproxy o una VPN sin cliente (cVPN), y no necesitan usar el plug-in de Citrix Gateway para establecer una VPN completa.
  - Para determinar que el almacén y todos los demás recursos de la red interna estén disponibles a través de un túnel de red privada virtual (VPN) con capa de sockets seguros (SSL), seleccione **Túnel VPN completo**. Los usuarios necesitan el plug-in de Citrix Gateway para establecer el túnel VPN.

  Al habilitar el acceso remoto al almacén, el método de autenticación **PassThrough desde Citrix Gateway** se habilita automáticamente. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes.

4. Si ha habilitado el acceso remoto, en la lista **Dispositivos Citrix Gateway**, seleccione las implementaciones a través de las que los usuarios pueden acceder al almacén. Las implementaciones previamente configuradas para este y otros almacenes están disponibles y se pueden seleccionar de la lista. Si quiere agregar otra implementación a la lista, haga clic en **Agregar**. De lo contrario, vaya al paso 14.
5. En la página Parámetros generales, especifique un **nombre simplificado** para el dispositivo Citrix Gateway que ayude a los usuarios a identificarlo.

   Los usuarios verán el nombre simplificado que especifique en la aplicación Citrix Workspace, de modo que debe incluir la información relevante en el nombre para ayudarlos a decidir si utilizar esa puerta de enlace o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de Citrix Gateway, de modo que los usuarios puedan identificar fácilmente la implementación más conveniente en función de su ubicación.
6. En **URL de Citrix Gateway**, escriba la combinación URL:puerto del servidor virtual de Citrix Gateway de la implementación. Si no especifica ningún puerto, se utiliza el puerto predeterminado `https://` de 443. No es necesario especificar el puerto 443 en la URL.
7. Seleccione el uso de Citrix Gateway a partir de las opciones disponibles.
   - **Autenticación y enrutamiento de HDX:** Citrix Gateway se usará para la autenticación y para el enrutamiento de las sesiones HDX.
   - **Solo autenticación:** Citrix Gateway se usará para la autenticación, no para el enrutamiento de las sesiones HDX.
   - **Solo enrutamiento de HDX:** Citrix Gateway se usará para enrutar sesiones HDX, no para la autenticación.
8. Para todas aquellas implementaciones en las que los recursos que ofrezcan Citrix Virtual Apps and Desktops o XenApp 6.5 estarán disponibles en el almacén, indique las direcciones URL de

Secure Ticket Authority (STA) de los servidores que ejecutan STA en la página **Secure Ticket Authority**. 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 Citrix Virtual Apps and Desktops o XenApp 6.5. Emite tíquets de sesión en respuesta a las solicitudes de conexión. Esos tíquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de Citrix Virtual Apps and Desktops o XenApp 6.5. Utilice la URL de STA correcta (como `HTTPS://` o `HTTP://`), según cómo estén configurados los Delivery Controllers. La dirección URL de STA también debe ser idéntica a la configurada en el dispositivo Citrix Gateway presente en el servidor virtual.

9. Elija el equilibrio de carga para Secure Ticket Authority. También puede especificar el intervalo de tiempo tras el cual se omitirá un STA que no responda.
10. Para garantizar que Citrix Virtual Apps and Desktops o XenApp 6.5 mantengan abiertas las sesiones desconectadas mientras la aplicación Citrix Workspace intenta volver a conectarse automáticamente, seleccione **Habilitar fiabilidad de la sesión**.
11. Si ha configurado varios STA y quiere que la fiabilidad de la sesión esté siempre disponible, seleccione **Solicitar tíquets de dos STA, si están disponibles**. StoreFront obtiene tíquets de sesión de dos STA diferentes, con lo que las sesiones de usuario no se interrumpen si un STA deja de estar disponible durante la sesión. Si, por algún motivo, StoreFront no puede establecer contacto con dos STA, vuelve a utilizar un solo STA.
12. En la página **Parámetros de autenticación**, escriba la **dirección IP del servidor virtual** (VIP) que tenga el dispositivo Citrix Gateway.

    Utilice la dirección IP privada para el servidor virtual de Citrix Gateway, en lugar de la dirección IP pública que está vinculada por NAT a la dirección IP privada. StoreFront suele identificar las puertas de enlace a través de sus URL. Si está utilizando GSLB (equilibrio de carga del servidor global), debe agregar la dirección IP virtual a cada puerta de enlace. Eso permite a StoreFront identificar varias puertas de enlace que utilizan la misma URL (nombre de dominio GSLB) como puertas de enlace distintas. Por ejemplo, el almacén puede tener configuradas tres puertas de enlace con la misma URL, como `https://gslb.domain.com`, pero cada una tendría direcciones IP virtuales únicas configuradas como 10.0.0.1, 10.0.0.2 y 10.0.0.3.
13. Si quiere agregar un dispositivo con Citrix Gateway, seleccione en la lista **Tipo de inicio de sesión** el método de autenticación configurado en el dispositivo para los usuarios de la aplicación Citrix Workspace.
    - 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**.

14. Si está configurando StoreFront para Citrix Gateway y quiere usar SmartAccess, debe escribir una **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 Citrix Gateway para verificar que las solicitudes recibidas desde Citrix Gateway provienen de ese dispositivo.

    Cuando se utilice GSLB, se recomienda que configure direcciones URL de respuesta únicas para cada una de las puertas de enlace de GSLB. StoreFront debe poder resolver cada una de las URL de respuesta únicas y recurrir a las direcciones IP virtuales privadas configuradas para cada uno de los servidores virtuales de puerta de enlace de GSLB. Por ejemplo, `emeagateway.domain.com`, `usgateway.domain.com` y `apacgateway.domain.com` deben recurrir a la dirección IP virtual de la puerta de enlace correcta.

15. Haga clic en **Crear** para agregar su dispositivo Citrix Gateway a la lista del cuadro de diálogo **Configurar parámetros de acceso remoto**.

    La información sobre la configuración de los dispositivos Citrix Gateway se guarda en el archivo de aprovisionamiento .cr del almacén. Eso permite que la aplicación Citrix Workspace envíe la solicitud de conexión pertinente al comunicarse con los dispositivos por primera vez.

16. Repita los pasos del 4 a 13, si fuera necesario, para agregar más dispositivos Citrix Gateway a la lista de dispositivos Citrix Gateway. Si habilita el acceso a través de varios dispositivos porque selecciona más de una entrada de la lista, especifique el **Dispositivo predeterminado** que se utilizará para acceder al almacén.

17. Haga clic en **Aceptar** para guardar la configuración y cerrar el cuadro de diálogo Configurar parámetros de acceso remoto.

la comprobación de listas de revocación de certificados (CRL)

March 2, 2020

Introducción

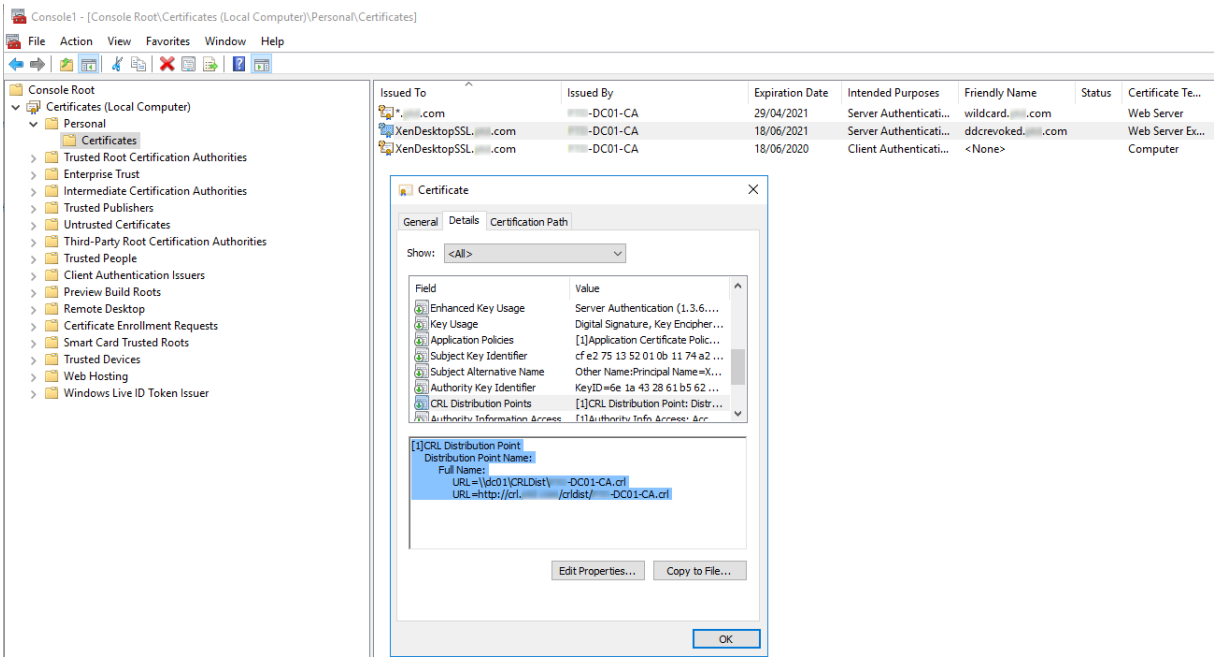
Puede configurar StoreFront para que este compruebe el estado de los certificados TLS que utilizan los utilizados los controladores de entrega de
CVAD mediante una lista de revocación de certificados (CRL) publicada.Es posible
que deba revocar el acceso a un certificado si:

- cree que la clave privada haya podido desvelarse
- la CA no es segura
- la afiliación ha cambiado
- el certificado se ha reemplazado

> **Nota:**
>
> Este tema solo es relevante cuando se utilizan conexiones HTTPS entre StoreFront y controladores de entrega de Citrix Virtual Apps and Desktops. Las conexiones HTTP a los controladores de entrega no requieren certificado, por lo que el parámetro -CertRevocationPolicy para el almacén, descrito aquí, no tiene ningún efecto.
>
> StoreFront admite la comprobación de revocación de certificados mediante extensiones de certificado de
> puntos de distribución de CRL (CDP) y
> listas de revocación de certificados (CRL) instaladas localmente. StoreFront solo admite listas CRL completas, por lo que no se admiten listas CLR delta.

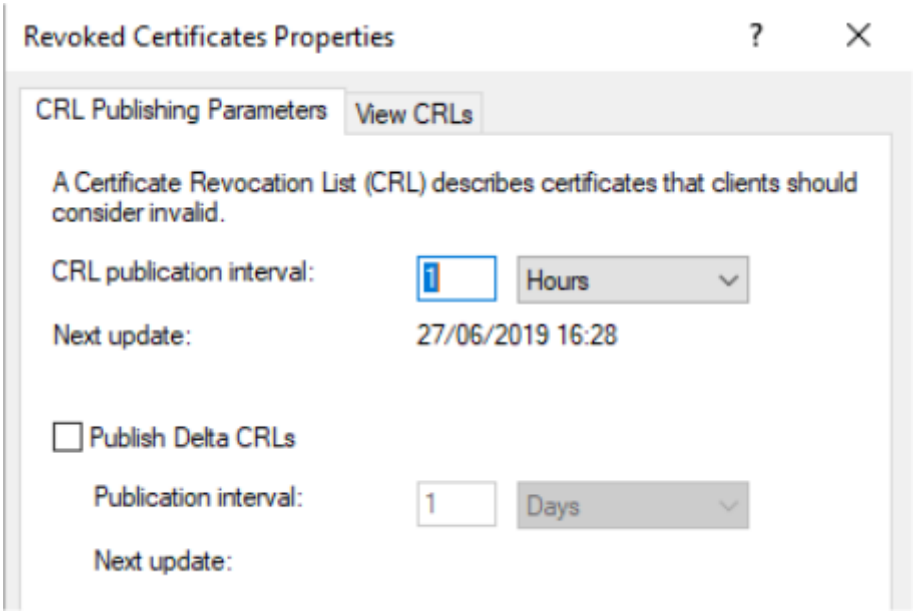
Extensiones de puntos de distribución CRL (CDP)

StoreFront no enumera los recursos de los controladores de
entrega provenientes de Citrix Virtual Apps and Desktops que utilizan certificados revocados cuyos números de serie
aparecen en la lista CRL publicada. Para detectar qué certificados se han revocado,
StoreFront debe poder acceder a la CRL publicada mediante una de las URL
definidas en las extensiones de certificado CDP.



Intervalo de publicación de CRL

Para que StoreFront detecte los certificados revocados en el Delivery Controller más rápidamente, reduzca el intervalo de publicación de CRL en la CA. Modifique las propiedades de la extensión de puntos de distribución de CRL para establecer un valor de intervalo de publicación CRL inferior adecuado a su infraestructura de clave pública.



Almacenamiento en caché de listas CRL del cliente

El cliente de infraestructura de clave pública de Windows almacena en caché las CRL localmente. Una CRL más reciente no se descarga hasta que la CRL almacenada localmente haya caducado.

Acceso de StoreFront a listas de revocación de certificados (CRL)

La comprobación de revocación de certificados depende de la capacidad de StoreFront para acceder a las listas CRL.
Tenga en cuenta cómo StoreFront se pone en contacto con el servidor web o la entidad de certificación (CA) que publica la CRL, y cómo StoreFront recibe las actualizaciones de CRL.

CA empresariales internas y certificados privados en los controladores de entrega

Para utilizar entidades CA y certificados privados, StoreFront necesita una CA de empresa debidamente configurada y una CRL publicada a la que pueda acceder sin salir de la organización ni la red interna. Consulte la documentación de Microsoft para obtener información sobre cómo configurar la CA de empresaria para publicar extensiones CDP. Puede que sea necesario volver a emitir todos los certificados que hubiera en los controladores de entrega que existieran antes de que la CA se configurara para incluir extensiones CDP.

Los servidores de StoreFront y Citrix Virtual Apps and Desktops suelen estar en redes privadas aisladas sin acceso a Internet. En este caso, se deben utilizar CA privadas.

CA públicas externas y certificados públicos en controladores de entrega

Los servidores de StoreFront y los controladores de entrega de Citrix Virtual Apps and Desktops pueden usar certificados emitidos por entidades de certificación públicas. StoreFront debe poder establecer contacto con el servidor web de la CA pública a través de Internet mediante la URL a la que se hace referencia en las extensiones CDP. Si StoreFront no puede descargar una copia de la CRL mediante una URL de CDP una vez que se haya revocado un certificado público, StoreFront no puede realizar la comprobación de CRL.

configuración de la directiva de revocación de certificados

Si quiere establecer la directiva de revocación de certificados para un almacén, utilice los cmdlets **Get-STFStoreFarmConfiguration** y **Set-STFStoreFarmConfiguration** de PowerShell para Citrix StoreFront. Tras ejecutar **Get-Help Set-STFStoreFarmConfiguration -detailed**, aparece la ayuda de PowerShell, con ejemplos de la opción -CertRevocationPolicy. Para obtener más información sobre estos cmdlets de PowerShell para StoreFront, consulte Módulos de PowerShell del SDK de Citrix StoreFront.

La opción **-CertRevocationPolicy** se puede establecer en los siguientes valores:

Parámetro	Descripción
NoCheck	StoreFront no comprueba el estado de revocación del certificado que haya presente en el controlador de entrega. StoreFront sigue enumerando los recursos provenientes de los controladores de entrega que utilizan certificados revocados. Esta es la opción predeterminada.
MustCheck	Esta es la opción más segura. StoreFront intenta obtener una CRL tras acceder a las URL a las que se hace referencia en las extensiones CDP del certificado en el Delivery Controller. StoreFront no enumera los recursos del Delivery Controller si la CRL no está disponible o si se ha revocado el certificado en uso en el Delivery Controller. La dirección URL puede apuntar a un servidor web interno si el certificado es privado o a un servidor web público de Internet si el certificado es emitido por una entidad de certificación pública.

Parámetro	Descripción
FullCheck	StoreFront intenta acceder a las URL publicadas en las extensiones CDP del certificado del controlador de entrega. Si StoreFront no consigue obtener una copia de la CRL a partir de las URL, sigue permitiendo la enumeración de recursos del Delivery Controller. Si StoreFront obtiene la CRL y se ha revocado el certificado del Delivery Controller, StoreFront no enumera los recursos. La dirección URL puede apuntar a un servidor web interno si el certificado es privado o a un servidor web público de Internet si el certificado es emitido por una entidad de certificación pública.
NoNetworkAccess	Solo se comprueban las CRL, que se han importado localmente en el almacén de certificados de Citrix Delivery Servers en el servidor de StoreFront. StoreFront no intenta ponerse en contacto con ninguna de las URL especificadas en las extensiones CDP. Si StoreFront no consigue obtener una copia local de la CRL, seguirá permitiendo la enumeración de recursos del Delivery Controller. Si StoreFront obtiene una copia local de la CRL proveniente del almacén de certificados de Citrix Delivery Servers y se ha revocado el certificado del Delivery Controller, StoreFront no enumera los recursos.

Configurar un almacén para la comprobación de la revocación de certificados

Para establecer la directiva de revocación de certificados para un almacén, abra PowerShell ISE con **Ejecutar como administrador** y, a continuación, ejecute los siguientes cmdlets de PowerShell. Si tiene
varios almacenes, repita este procedimiento en todos ellos. -CertRevocationPolicy
es una configuración a nivel de almacén que afecta a todos los Delivery Controllers configurados para

el
almacén especificado en $StoreVirtualPath.

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

Para comprobar que la configuración se ha aplicado correctamente o para ver la configuración actual de
-CertRevocationPolicy, ejecute lo siguiente:

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

Usar CRL importadas localmente en el servidor de StoreFront

Se pueden usar CRL importadas localmente, aunque Citrix no lo recomienda porque:

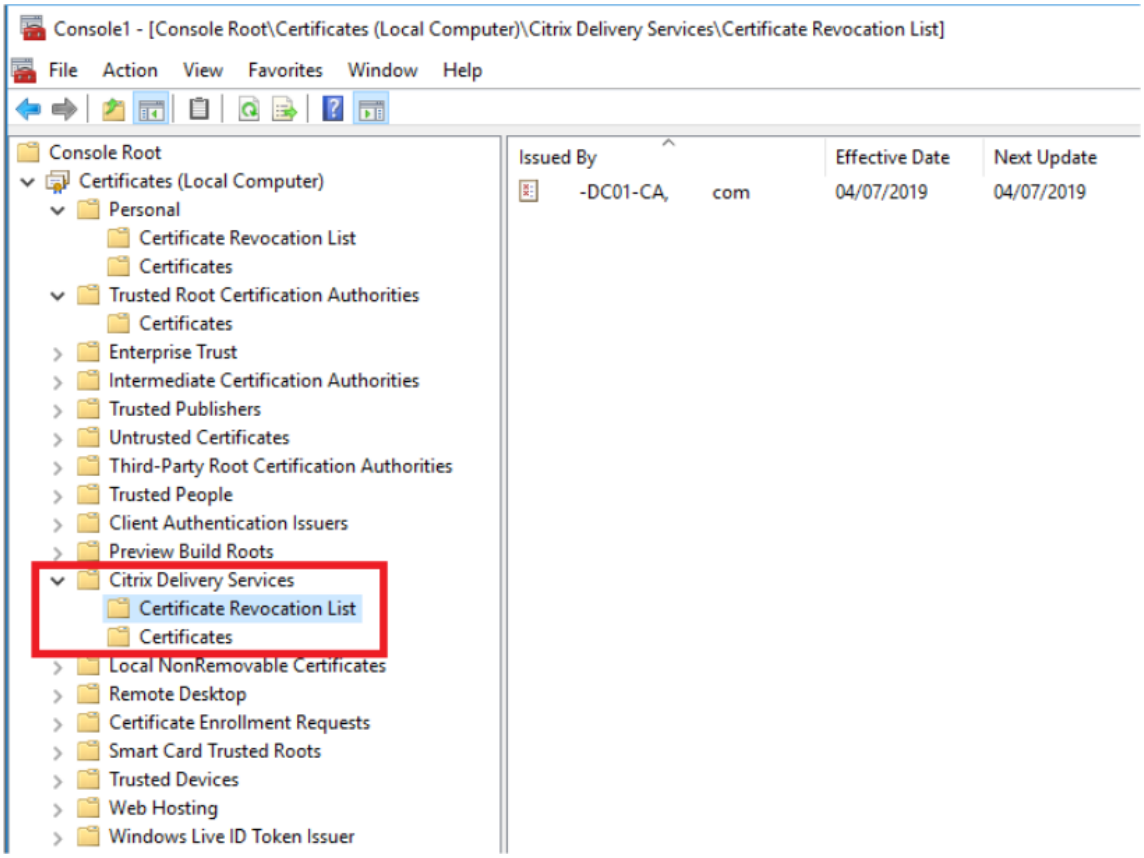
- Son difíciles de administrar y actualizar en grandes implementaciones empresariales, donde puede tratarse de varios grupos de servidores de StoreFront.
- La actualización manual de las CRL en cada servidor de StoreFront, cada vez que se revoca un certificado, es mucho menos eficiente que usar extensiones CDP y CRL publicadas en todo el dominio de Active Directory.

El uso de CRL instaladas localmente o actualizadas se puede utilizar si -CertRevocationPolicy se establece en "NoNetworkAccess" y dispone de los medios para distribuir la CRL de manera eficiente a todos los servidores de StoreFront.

Para utilizar CLR importadas localmente

1. Copie la CRL en el escritorio del servidor de StoreFront. Si el servidor de StoreFront forma parte de un grupo de servidores, cópiela a todos los servidores de StoreFront del grupo.
2. Abra el complemento MMC y seleccione **Archivo > Agregar o quitar complementos > Certificados > Cuenta de equipo > Almacén de certificados de Citrix Delivery Services**.
3. Haga clic con el botón secundario y seleccione **Todas las tareas > Importar** y, a continuación, vaya al archivo .CRL

y elija **Seleccionar todos los archivos > Abrir > Colocar todos los certificados en el siguiente almacén > Citrix Delivery Services**.



Para agregar la CRL al almacén de certificados de Citrix Delivery Services mediante PowerShell o la línea de comandos

1. Inicie sesión en StoreFront y copie el archivo .CRL al escritorio del usuario actual.
2. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.
3. Ejecute lo siguiente:

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

Si la operación se lleva a cabo correctamente, el resultado es el siguiente:

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


Puede utilizar este comando como ejemplo para distribuir automáticamente la CRL a todos los servidores de StoreFront de su implementación mediante scripts.

Autenticación XML mediante Delivery Controllers

Puede configurar StoreFront para delegar la autenticación de usuarios en los Delivery Controllers de Citrix Virtual
Apps and Desktops. Los usuarios no pueden iniciar sesión en
StoreFront si se ha revocado el certificado del Delivery Controller. Este
comportamiento es preferible ya que los usuarios de Active Directory no deberían poder iniciar sesión en
StoreFront si se ha revocado el certificado del Delivery Controller de
Citrix Virtual Apps and Desktops, que es lo que los autentica.

Para delegar la autenticación de usuarios a los Delivery Controllers

1. Configure el almacén para la revocación de certificados tal y como se describe en la sección anterior, Configurar un almacén para la comprobación de la revocación de certificados.
2. Configure el Delivery Controller para que use HTTPS y siga el procedimiento descrito en Autenticación basada en el servicio XML.

Configurar un servicio de autenticación XML para la comprobación de la revocación de certificados

Estos pasos solo son necesarios si utiliza la autenticación XML en su implementación.

> **Nota:**
>
> StoreFront admite dos modelos para asignar almacenes a un
> servicio de autenticación. El método recomendado es una asignación individual entre almacén y
> servicio de autenticación. En este caso, debe seguir los pasos de esta sección
> en todos los almacenes y sus respectivos servicios de autenticación.
>
> Compruebe que el modo de revocación de certificados tiene el mismo valor
> tanto en el almacén como en el servicio de autenticación. Como alternativa, si la
> configuración de la autenticación es idéntica para todos los almacenes, se pueden
> configurar varios almacenes para que compartan un único servicio de autenticación.

Los cmdlets de PowerShell del servicio de autenticación no tienen el equivalente de **Set-STFStoreFarmConfiguration**, por lo que se necesita un estrategia ligeramente diferente con PowerShell. Utilice la misma configuración de la directiva de revocación de certificados descrita en la sección anterior.

1. Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

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

2. Seleccione el servicio de almacén, el servicio de autenticación y el Delivery Controller para que se utilicen en la autenticación XML. Compruebe que el Delivery Controller ya está configurado para el almacén.

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

3. Modifique directamente la propiedad CertRevocationPolicy del servicio de autenticación.

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

4. Confirme que ha establecido el modo de revocación de certificados correcto.

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

Errores previsibles del Visor de eventos de Windows

Cuando la comprobación CRL está habilitada, se notifican errores en el Visor de eventos de Windows en el servidor de StoreFront.

Para abrir el Visor de eventos:

- En el servidor de StoreFront, escriba **Run**.
- Escriba **eventvwr** y luego pulse Intro.
- En Aplicaciones y servicios, busque eventos de Citrix Delivery Services.

Ejemplo de error: El almacén no puede contactar con un Delivery Controller mediante un certificado revocado

```
No se pudo establecer una conexión SSL: Ocurrió un error durante la
    autenticación SSL
Criptografía: Acceso denegado.

Este mensaje fue enviado desde Citrix XML Service en la dirección
https://deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.

No se pudo contactar con el servicio Citrix XML Service especificado
    por lo que ha sido
eliminado temporalmente de la lista de servicios activos.
```

Ejemplo de error: En Receiver para Web, si el usuario no puede iniciar sesión por un error en la autenticación XML

```
Se recibió una respuesta inesperada durante el proceso de autenticación
    .

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

Error general de autenticación

ExplicitResult.State: 5

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

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
    GetExplicitAuthResult(ActionType
```



```
18  type, Dictionary‘2 postParams)
```

Configurar dos almacenes de StoreFront para compartir un almacén de datos de suscripción común

January 6, 2020

El proceso de instalación de StoreFront instala localmente un almacén de datos de Windows en cada servidor de StoreFront para mantener sus datos de suscripción. En los entornos de grupos de servidores de StoreFront, cada servidor también mantiene una copia de los datos de suscripción que emplea su almacén. 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 almacén. Cada almacén de datos de suscripción se actualiza de forma independiente con respecto a otros almacenes.

Es común que los administradores configuren StoreFront con dos almacenes diferentes allá donde se necesiten diferentes parámetros de configuración. Uno de los almacenes es para el acceso externo a recursos a través de Citrix Gateway y el otro es para el acceso interno a través de la red LAN de la organización. Puede configurar almacenes “externos” e “internos” para compartir un mismo almacén de datos de suscripción con solo realizar un pequeño cambio en el archivo web.config del almacén.

En la situación predeterminada con dos almacenes y sus correspondientes almacenes de datos de suscripción, el usuario debe suscribirse al mismo recurso dos veces. Si se configuran ambos almacenes para compartir una misma base de datos de suscripción, puede mejorar y simplificar la experiencia de los usuarios itinerantes 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 el almacén “externo” o el “interno” cuando se suscriben por primera vez a un nuevo recurso.

- Cada almacén 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.

```
<clientEndpoint uri=”net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<
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 almacenes compartan un almacén de datos de suscripción, solo necesita apuntar un almacén al punto final del servicio de suscripción del otro almacén. Si se trata de la implementación de

un grupo de servidores, todos los servidores tienen definidos pares idénticos de almacenes y copias idénticas del almacén de datos que comparten.

> Nota:
>
> Los Controllers de Citrix Virtual Apps and Desktops 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 se admite cuando los dos almacenes se encuentran en el mismo servidor de 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:

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

2. Cambie el punto final del almacén externo para que coincida con el punto final del almacén interno:

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

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

Ahora, ambos almacenes están configurados para compartir el almacén de datos de suscripción del almacén interno.

Administrar datos de suscripción a un almacén

June 24, 2019

Puede administrar los datos de suscripción a un almacén 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.

Purgar datos de suscripción

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

1. Detenga el servicio de suscripciones a almacenes de Citrix en el servidor de StoreFront. Mientras el servicio de suscripciones a almacenes de Citrix esté en ejecución, no se puede eliminar datos de suscripción de ningún almacén.
2. Busque la carpeta de suscripción al almacén, ubicada en el servidor de StoreFront: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. Elimine el contenido de la carpeta de suscripción al almacén, pero no elimine la carpeta en sí.
4. Vuelva a iniciar el servicio de suscripciones a almacenes de Citrix en el servidor de StoreFront.

En StoreFront 3.5 o versiones posteriores, puede utilizar el siguiente script de PowerShell para purgar los datos se suscripción a un almacén. 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.

```
function Remove-SubscriptionData

{

        [CmdletBinding()]

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

```



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

Exportar datos de suscripción

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

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
      yourstore>"
2
3 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 de 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 de StoreFront, exporte los datos de todos los servidores del grupo y compárelos para ver las diferencias.

Restaurar datos de suscripción

Use Restore-STFStoreSubscriptions para sobrescribir los datos existentes de suscripción. Puede restaurar los datos de suscripción a un almacén 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://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Restore-STFStoreSubscriptions/

Restaurar datos en un solo servidor de StoreFront

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

Restaurar datos en un grupo de servidores de StoreFront

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

Ejemplo: implementación de un grupo de tres servidores de 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 de suscripción a almacenes en los servidores de 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 de StoreFrontB y C. Esto 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 de suscripción a almacenes 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 de 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.

Importar datos de suscripción

Use **Import-STFStoreSubscriptions** cuando no hay datos de suscripción al almacén. Este cmdlet también permite que los datos de suscripción se transfieran de un almacén a otro, además de permitir que esos datos se importen a servidores de StoreFront recién aprovisionados.

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

Para obtener más información sobre Import-STFStoreSubscriptions, consulte https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Import-STFStoreSubscriptions/

Detalles 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:

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

donde:

- `<user-identifier>`: Requerido. Una secuencia de caracteres que identifica al usuario. Es el identificador de seguridad de Windows perteneciente al usuario.
- `<resource-id>`: Requerido. Una secuencia de caracteres que identifica los recursos suscritos.
- `<subscription-id>`: Requerido. 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>`: Requerido. El estado de la suscripción: suscrito o no suscrito.
- `<property-name>` y `<property-value>`: Opcional. Una secuencia de cero o más pares de valores de nombre y valor. Estos representan propiedades asociadas a la suscripción por parte de un cliente StoreFront (suele ser una aplicación Citrix Workspace). 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 de 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 archivos .txt importados y exportados

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 Store Subscription

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 de StoreFront.

Ver contadores de suscripción mediante PowerShell

```
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"
```

Almacenar datos de suscripción mediante Microsoft SQL Server

March 2, 2020

> **Nota:**
>
> En este documento, se presupone que tiene conocimientos básicos de MS SQL Server y las consultas T-SQL. Los administradores deben estar familiarizados con la configuración, uso y administración de SQL Server antes de intentar seguir este documento.

Introducción

ESENT es un motor de base de datos transaccional incrustable que se puede usar con Windows. Todas las versiones de StoreFront son compatibles de forma predeterminada con el uso de una base de datos ESENT integrada. También pueden conectarse a una instancia de Microsoft SQL Server si el almacén está configurado para utilizar una cadena de conexión SQL.

La principal ventaja de cambiar StoreFront para uso de SQL, en lugar de ESENT, es que las instrucciones de actualización T-SQL le permiten administrar, modificar o eliminar registros de suscripción.

Si utiliza SQL, no es necesario exportar, modificar ni volver a importar todos los datos de suscripción de ESENT cada vez que se hagan cambios menores en estos.

Para migrar los datos de suscripción de ESENT a Microsoft SQL Server, los datos planos de ESENT exportados desde StoreFront deben transformarse a un formato de fácil lectura para la importación en bloque en SQL. Para nuevas implementaciones sin nuevos datos de suscripción, este paso no es necesario. El paso de transformación de los datos solo es necesario completarlo una vez. En este artículo, se describe la configuración compatible que puede utilizarse en todas las versiones de StoreFront, a partir de la versión 3.5, en la que se que introdujo el SDK de PowerShell -STF al que se hace referencia.

> **Nota:**
>
> Los fallos en la conexión a la instancia de SQL Server utilizada por StoreFront para almacenar los datos de suscripción debido a interrupciones en la red no hacen inutilizable la implementación de StoreFront. Las interrupciones solo afectan temporalmente a la experiencia de usuario: los usuarios no pueden agregar, quitar o ver sus recursos favoritos hasta que se restaura la conexión con el servidor SQL. Los recursos sí se pueden enumerar e iniciar durante la interrupción. El comportamiento previsto es el mismo que si el servicio Citrix Subscription Store se detuviera durante el uso de ESENT.
>
> **Sugerencia:**
>
> Los recursos configurados con las palabras clave Auto o Mandatory funcionan de la misma manera cuando se utilizan con ESENT o SQL. Los nuevos registros de suscripción de SQL se crean automáticamente cuando un usuario inicia sesión por primera vez si se incluye cualquiera de esas dos palabras clave en los recursos del usuario.

Ventajas de ESENT y SQL Server

ESENT	SQL
Predeterminado y no requiere configuración adicional para usar StoreFront “estándar”.	Mucho más manejable, y los datos de suscripción se pueden manipular o actualizar fácilmente mediante consultas T-SQL. Permite eliminar o actualizar registros por usuario. Permite hacer recuento de registros por aplicación, Delivery Controller o usuario. Ofrece un medio fácil para eliminar datos de usuario innecesarios cuando los usuarios dejan la empresa/organización. Ofrece una manera fácil de actualizar las referencias de los Delivery Controllers, por ejemplo, cuando el administrador cambia a uso de agregación o se aprovisionan nuevos Delivery Controllers.
Más fácil de configurar la replicación entre diferentes grupos de servidores mediante la sincronización de suscripciones y las programaciones de extracción. Consulte Configurar la sincronización de suscripciones	Separado de StoreFront, por lo que no es necesario hacer copia de seguridad de los datos de suscripción antes de actualizar StoreFront, ya que los datos se conservan en un servidor SQL independiente. La copia de seguridad de las suscripciones es independiente de StoreFront y utiliza estrategias y mecanismos de copia de seguridad de SQL.
SQL no es necesario cuando no se necesita administrar suscripciones. Si los datos de suscripción nunca necesitarán actualizarse, es probable que ESENT satisfaga las necesidades del cliente.	Una sola copia de los datos de suscripción que comparten todos los miembros del grupo de servidores, lo que reduce la probabilidad de que haya discrepancias en los datos de los distintos servidores o problemas de sincronización de datos.

Desventajas de ESENT y SQL Server

ESENT	SQL
No es fácil administrar los datos de suscripción de forma sencilla y granular. Requiere que la manipulación de las suscripciones se haga en archivos .txt exportados. Obliga a exportar y volver a importar toda la base de datos de suscripción. Posibilidad de tener que cambiar miles de registros mediante técnicas de búsqueda y reemplazo, que requieren mucho esfuerzo y son propensas a errores.	Requiere infraestructura y conocimientos básicos de SQL. Puede requerir la compra de una licencia SQL, lo que aumenta el coste total de propiedad de la implementación de StoreFront. Aun así, es posible compartir una instancia de base de datos de Citrix Virtual Apps and Desktops con StoreFront para reducir los costes.
Es necesario mantener una copia de la base de datos ESENT en cada servidor de StoreFront de un grupo de servidores. En raras ocasiones, esta base de datos puede desincronizarse dentro de un grupo de servidores o entre diferentes grupos de servidores.	Replicar datos de suscripción entre grupos de servidores no es una tarea de implementación trivial. Requiere múltiples instancias de SQL y replicación de transacciones entre cada una de ellas para cada centro de datos. Esto requiere unos conocimientos especializados de MS SQL.
	Requiere la migración de datos de ESENT y la transformación a un formato de fácil lectura para SQL. Este proceso solo se requiere una vez.
	Es posible que se necesiten licencias y servidores Windows adicionales.
	Pasos adicionales para implementar StoreFront.

Escenarios de implementación

> **Nota:**
>
> Cada almacén configurado en StoreFront requiere una base de datos ESENT o una base de datos de Microsoft SQL para compatibilidad con suscripciones de usuario. El método de almacenamiento de los datos de suscripción se establece en el nivel de almacén dentro de StoreFront.

Citrix recomienda que todas las bases de datos de almacenes residan en la misma instancia de Microsoft SQL Server para reducir la complejidad de la administración y la posibilidad de una configuración incorrecta.

Varios almacenes pueden compartir la misma base de datos, siempre que estén configurados para usar una cadena de conexión idéntica. No importa si utilizan Delivery Controllers diferentes. La

desventaja de que varios almacenes compartan una misma base de datos es que no hay forma de saber a qué almacén corresponde cada registro de suscripción.

Una combinación de los dos métodos de almacenamiento de datos es técnicamente posible en una misma implementación de StoreFront con varios almacenes Es posible configurar un almacén para uso de ESENT y otro para uso de SQL. Esto no se recomienda debido a la mayor complejidad de la administración y a la posibilidad de una configuración incorrecta.

Hay cuatro escenarios que puede usar para almacenar datos de suscripción en SQL Server:

Escenario 1: Un único servidor o grupo de servidores de StoreFront con ESENT (predeterminado)

De forma predeterminada, todas las versiones de StoreFront a partir de la versión 2.0 utilizan una base de datos ESENT plana para almacenar y replicar datos de suscripción entre miembros de un grupo de servidores. Cada miembro del grupo de servidores mantiene una copia idéntica de la base de datos de suscripción, que se sincroniza con todos los demás miembros del grupo. Este escenario no requiere pasos de configuración adicionales. Además, es adecuado para la mayoría de los clientes que no prevén cambios frecuentes en los nombres de los Delivery Controllers o que no necesitan realizar tareas de administración con frecuencia en los datos de suscripción, como eliminar o actualizar suscripciones de usuario antiguas.

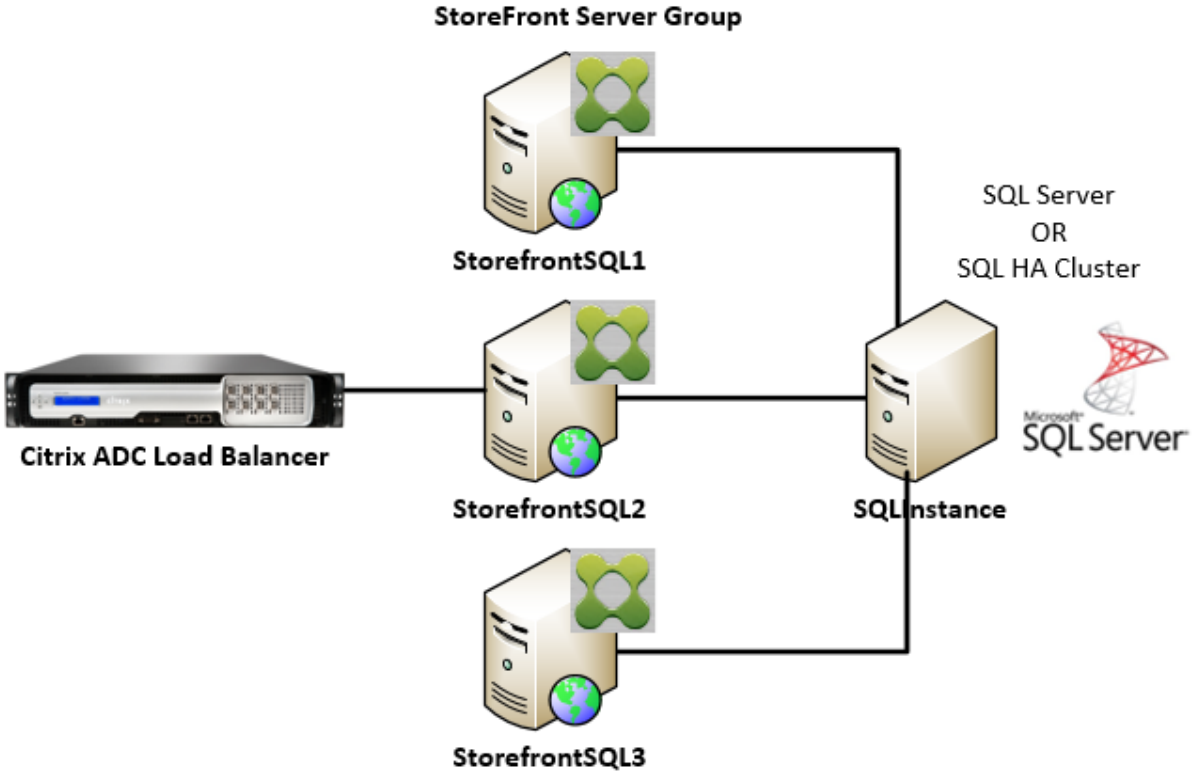
Escenario 2: Un único servidor de StoreFront y una instancia local de Microsoft SQL Server

StoreFront utiliza una instancia de SQL Server instalada localmente y ambos componentes residen en el mismo servidor. Este escenario es adecuado para una implementación simple de StoreFront en la que los clientes podrían necesitar hacer cambios frecuentes en los nombres de los Delivery Controllers o realizar tareas de administración con frecuencia en los datos de suscripción, como eliminar o actualizar suscripciones de usuario antiguas, pero no requieren una implementación de StoreFront de alta disponibilidad. Citrix no recomienda este escenario para grupos de servidores, ya que da lugar a un punto único de error en el miembro del grupo de servidores que aloja la instancia de base de datos de Microsoft SQL. Este escenario no es adecuado para implementaciones en grandes empresas.

Escenario 3: Un grupo de servidores de StoreFront y una instancia dedicada de Microsoft SQL Server configurada para alta disponibilidad (recomendado)

Todos los miembros del grupo de servidores de StoreFront se conectan a la misma instancia dedicada de Microsoft SQL Server o clúster de conmutación por error SQL. Este es el modelo más adecuado para implementaciones en grandes empresas, en las que los administradores de Citrix desean realizar cambios frecuentes en los nombres de los Delivery Controllers o realizar tareas de administración

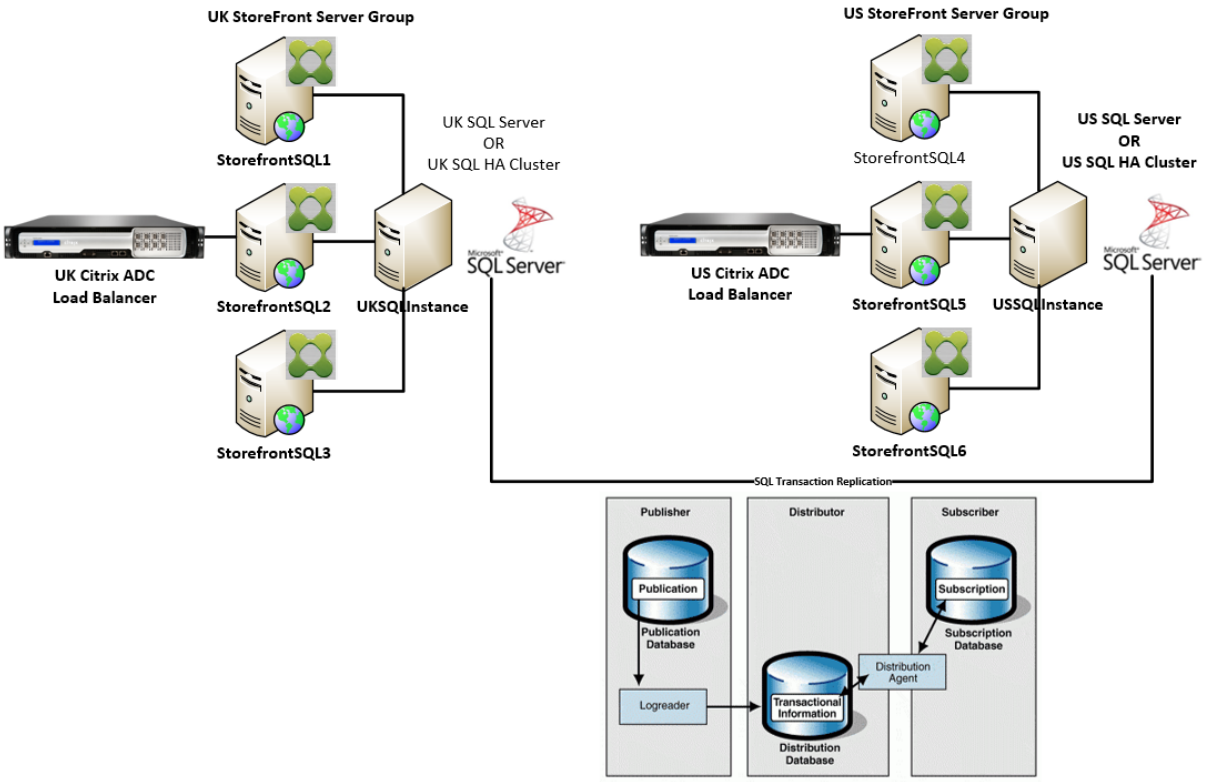
frecuentes en los datos de suscripción, como eliminar o actualizar suscripciones de usuario antiguas y requieren alta disponibilidad.



Escenario 4: Varios grupos de servidores de StoreFront y una instancia dedicada de Microsoft SQL Server en cada centro de datos para cada grupo de servidores

> **Nota:**
>
> Esta es una configuración avanzada. Inténtelo solo si es un administrador de SQL Server experimentado, está familiarizado con la replicación de transacciones y tiene las competencias necesarias para implementarlo correctamente.

Es igual que el escenario 3, pero se extiende a situaciones en las que se requieren varios grupos de servidores de StoreFront en diferentes centros de datos remotos. Los administradores de Citrix pueden elegir sincronizar los datos de suscripción entre diferentes grupos de servidores del mismo centro de datos o de diferentes centros de datos. Cada grupo de servidores del centro de datos se conecta a su propia instancia dedicada de Microsoft SQL Server para optimizar la redundancia, la conmutación por error y el rendimiento. Este escenario requiere una infraestructura y configuración de servidores Microsoft SQL extra considerables. Confía plenamente en la tecnología de Microsoft SQL para replicar los datos de suscripción y las transacciones SQL.



Recursos

Puede descargar los siguientes scripts de https://github.com/citrix/sample-scripts/tree/master/storefront como ayuda:

Scripts de configuración

- **Set-STFDatabase.ps1**: establece la cadena de conexión MS SQL para cada almacén. Se ejecuta en el servidor de StoreFront.
- **Add-LocalAppPoolAccounts.ps1**: concede a los grupos de aplicaciones locales del servidor de StoreFront acceso de lectura y escritura a la base de datos SQL. Se ejecuta para el escenario 2 en el servidor SQL.
- **Add-RemoteSFAccounts.ps1**: concede a todos los servidores de StoreFront de un grupo de servidores acceso de lectura y escritura a la base de datos SQL. Se ejecuta para el escenario 3 en el servidor SQL.
- **Create-StoreSubscriptionsDB-2016.sql**: crea el esquema y la base de datos SQL. Se ejecuta en el servidor SQL.

Scripts de transformación e importación de datos

- **Transform-SubscriptionDataForStore.ps1**: exporta y transforma los datos de suscripción existentes en ESENT a un formato de fácil lectura para importación en SQL.
- **Create-ImportSubscriptionDataSP.sql**: crea un procedimiento almacenado para importar los datos transformados con Transform-SubscriptionDataForStore.ps1. Ejecute este script una vez en el servidor SQL, después de haber creado el esquema de base de datos con Create-StoreSubscriptionsDB-2016.sql.

Configurar el grupo de seguridad local del servidor de StoreFront en SQL Server

Escenario 2: Un único servidor de StoreFront y una instancia local de Microsoft SQL Server

Cree un grupo de seguridad local llamado `<SQLServer>\StoreFrontServers` en el servidor Microsoft SQL y agregue las cuentas virtuales para `IIS APPPOOL\DefaultAppPool` y `IIS APPPOOL\Citrix Receiver for Web` para permitir que la instancia de StoreFront instalada localmente pueda leer y escribir en SQL. A este grupo de seguridad se hace referencia en el script .SQL que crea el esquema de base de datos de suscripciones del almacén, por lo que deberá asegurarse de que el nombre del grupo coincide.

Puede descargar el script Add-LocalAppPoolAccounts.ps1 como ayuda.

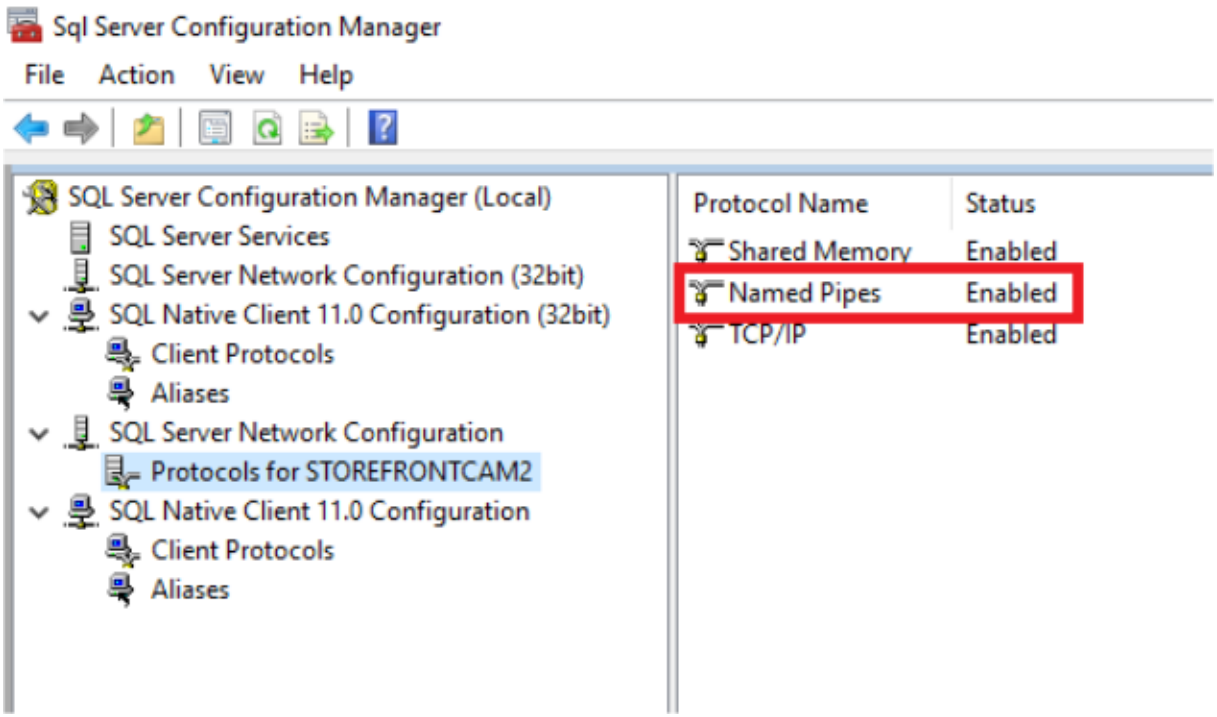
Instale StoreFront antes de ejecutar el script *Add-LocalAppPoolAccounts.ps1*. El script depende de la capacidad de localizar la cuenta virtual de IIS `IIS APPPOOL\Citrix Receiver for Web`, que no existe hasta que StoreFront se ha instalado y configurado. `IIS APPPOOL\DefaultAppPool` se crea automáticamente al instalar el rol de servidor web de IIS.

```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

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

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

else
{

Write-Host "Creating $LocalGroupName local security group" -
    ForegroundColor "Yellow"
```



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

Habilite las canalizaciones con nombre en su instancia SQL local con Administrador de configuración de SQL Server. Las canalizaciones con nombre son necesarias para la comunicación entre procesos entre StoreFront y SQL Server.

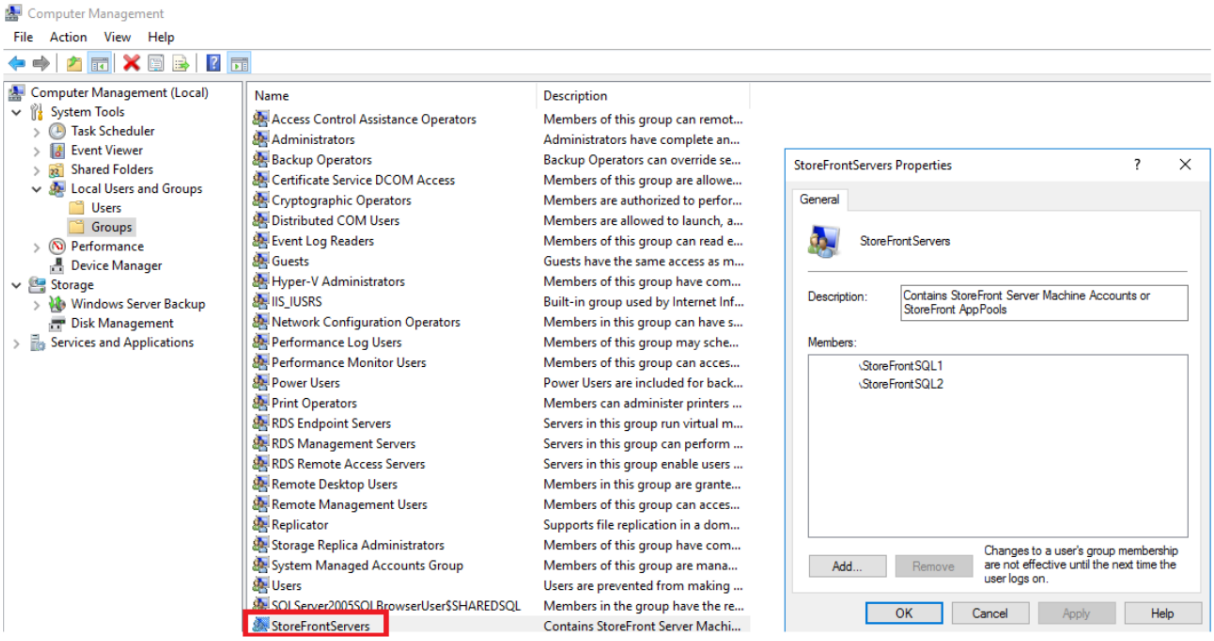


Asegúrese de que las reglas del firewall de Windows están configuradas correctamente para permitir conexiones de SQL Server a través de un puerto específico o de puertos dinámicos. Consulte la documentación de Microsoft para saber cómo hacerlo en su entorno.

> **Sugerencia:**
>
> Si se produce un error en la conexión a la instancia SQL local, compruebe que localhost o <hostname> utilizado en la cadena de conexión se resuelve en la dirección IPv4 correcta. Windows podría intentar usar IPv6 en lugar de IPv4, y la resolución DNS de localhost podría devolver ::1 en lugar de la dirección IPv4 correcta del servidor de StoreFront y SQL. Puede ser necesario inhabilitar completamente la pila de red IPv6 en el servidor host para resolver este problema.

Escenario 3: Un grupo de servidores de StoreFront y una instancia dedicada de Microsoft SQL Server

Cree un grupo de seguridad local llamado <SQLServer>\StoreFrontServers en el servidor Microsoft SQL y agregue todos los miembros del grupo de servidores de StoreFront. A este grupo de seguridad se hace referencia más adelante en el script **Create-StoreSubscriptionsDB-2016.sql** que crea el esquema de base de datos de suscripciones dentro de SQL.



Agregue todas las cuentas de equipo de dominio del grupo de servidores de StoreFront al grupo <SQLServer>\StoreFrontServers. Solo las cuentas de equipo de dominio de servidor de StoreFront enumeradas en el grupo podrán leer y escribir registros de suscripción en SQL si el servidor SQL utiliza la autenticación de Windows. La siguiente función de PowerShell, proporcionada en el script Add-RemoteSFAccounts.ps1, crea el grupo de seguridad local y le agrega dos servidores de StoreFront denominados StoreFrontSQL1 y StoreFrontSQL2.

```
function Add-RemoteSTFMachineAccounts
{

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

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

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

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

```



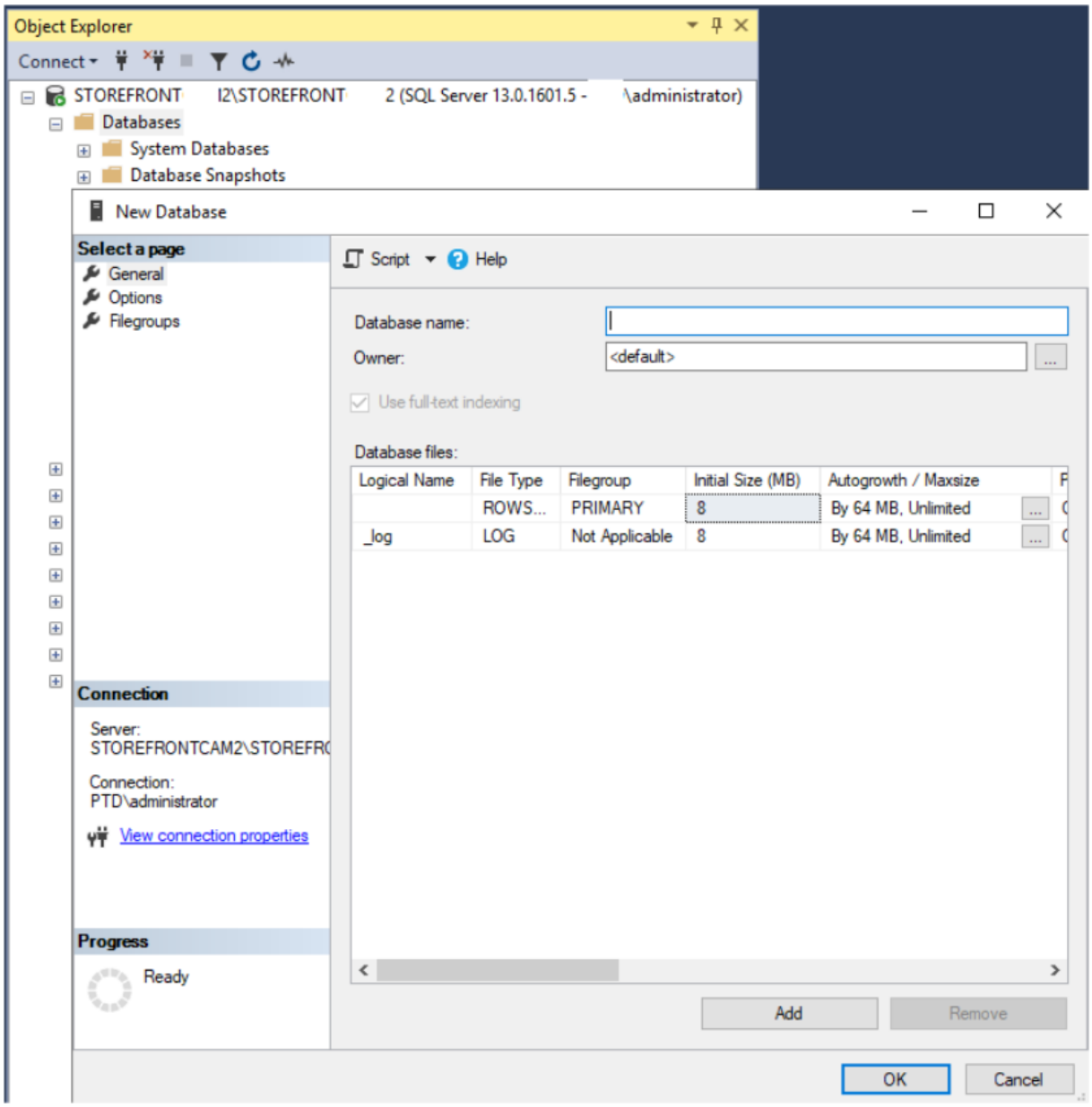
```
19 else
20 {
21
22     Write-Host ”Creating $LocalGroupName local group” -ForegroundColor
       ”Yellow”
23
24     # Create Local Security Group
25     $Computer = [ADSI]”WinNT://$env:ComputerName,Computer”
26     $LocalGroup = $Computer.Create(”group”,$LocalGroupName)
27     $LocalGroup.setinfo()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

Configurar el esquema de base de datos de suscripciones en Microsoft SQL Server para cada almacén

Cree una instancia con nombre en el servidor Microsoft SQL para uso en StoreFront. Establezca la ruta de acceso en el script .SQL para que se corresponda con el lugar donde está instalada la versión de SQL o donde se almacenan sus archivos de base de datos. El script de ejemplo Create-StoreSubscriptionsDB-2016.sql utiliza SQL Server 2016 Enterprise.

Haga clic con el botón derecho del mouse en **Bases de datos** y seleccione **Nueva base de datos** para

crear una base de datos vacía con SQL Server Management Studio (SSMS).



Introduzca un **nombre de base de base de datos** que coincida con el de su almacén o elija otro nombre, como *STFSubscriptions*.

Antes de ejecutar el script, para cada almacén de la implementación de StoreFront, modifique las referencias del script de ejemplo para que coincidan con las implementaciones de StoreFront y SQL. Por ejemplo, modifique:

- Asigne un nombre a cada base de datos que cree, de manera que coincida con el nombre del almacén de StoreFront en `USE [STFSubscriptions]`.
- Establezca la ruta de acceso a los archivos .mdf y .ldf de la base de datos donde quiere almace-

nar esta.

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

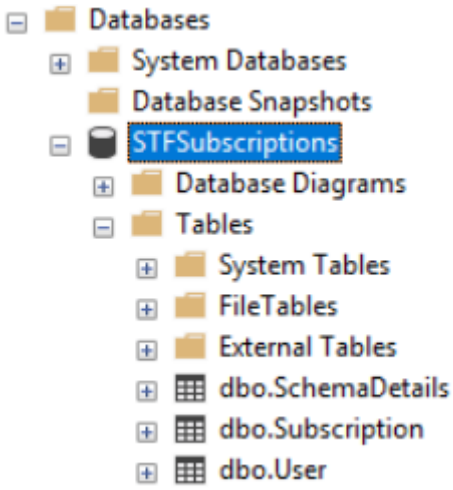
```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\
STFSubscriptions.ldf
```

- Establezca la referencia al nombre de su servidor SQL dentro del script:

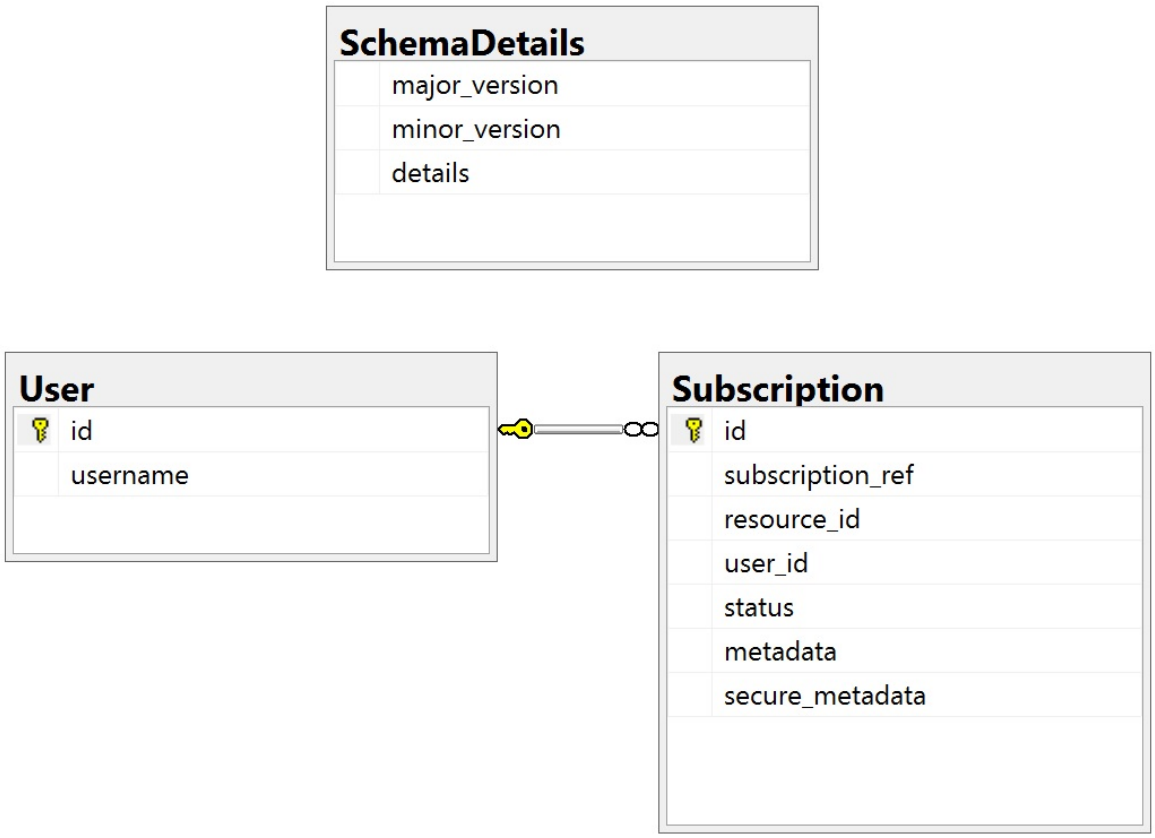
```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;
```

```
ALTER LOGIN [SQL2016\StoreFrontServers]
```

Ejecute el script. Después de configurar correctamente el esquema, se crean tres tablas de base de datos: *SchemaDetails*, *Subscription*y *User*.



El siguiente diagrama de base de datos muestra el esquema de base de datos de suscripciones que crea el script *Create-StoreSubscriptionsDB-2016.sql* :



Configurar la cadena de conexión de SQL Server para cada almacén de StoreFront

Caso 1

> **Sugerencia:**
>
> Los datos de suscripción originales almacenados en disco en la base de datos ESENT no se destruyen ni eliminan. Si decide revertir de Microsoft SQL Server a ESENT, es posible quitar la cadena de conexión del almacén y volver a utilizar los datos originales. Las suscripciones adicionales que se crearon mientras SQL estaba en uso para el almacén no existirán en ESENT, y los usuarios no podrán ver estos nuevos registros de suscripción. Todos los registros de suscripciones originales seguirán estando presentes.

Para volver a habilitar suscripciones ESENT en un almacén

Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

Utilice la opción **-UseLocalStorage** para especificar el almacén en el que quiere volver a habilitar las suscripciones ESENT:


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

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

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

Escenarios 2, 3 y 4

Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

Especifique el almacén para el que quiere establecer una cadena de conexión para usar **$StoreVirtualPath**

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

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

O BIEN

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

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


Repita el proceso para cada almacén de la implementación si quiere configurarlos todos para que utilicen una cadena de conexión SQL.

Migrar datos existentes de ESENT a Microsoft SQL Server

Para migrar los datos existentes de ESENT a SQL se requiere un proceso de transformación de los datos en dos pasos. Se proporcionan dos scripts para ayudarle a realizar esta operación, que se ejecuta una sola vez. Si la cadena de conexión en StoreFront y la instancia SQL están correctamente configuradas, todas las nuevas suscripciones se crean automáticamente en SQL en el formato correcto. Después de la migración, los datos históricos de suscripción de ESENT se transforman a un formato SQL y los usuarios también pueden ver sus recursos de suscripción previos.

Ejemplo: cuatro suscripciones SQL para el mismo usuario de dominio

Paso 1. Utilice el script Transform-SubscriptionDataForStore.ps1 para convertir los datos de ESENT a un formato de fácil lectura en SQL para la importación en bloque

Inicie sesión en el servidor de StoreFront para el que quiere transformar los datos de ESENT.

Cualquier miembro de un grupo de servidores es adecuado, siempre que todos contengan el mismo número de registros de suscripción.

Abra PowerShell ISE y seleccione **Ejecutar como administrador**.

Ejecute el script Transform-SubscriptionDataForStore.ps1, que exporta un archivo `<StoreName>.txt` de la base de datos ESENT al escritorio del usuario actual.

El script de PowerShell proporciona comentarios detallados sobre cada fila de suscripción que se procesa, a fin de ayudar a la depuración y evaluar el éxito de la operación. Esta operación puede tardar mucho tiempo en procesarse.

Los datos transformados se registran en `<StoreName>SQL.txt`, en el escritorio del usuario actual, una vez finalizado el script. El script resume el número de registros de usuario únicos y el número total de suscripciones procesadas.

Repita este proceso para cada almacén que desee migrar a SQL Server.

Paso 2. Utilice un procedimiento almacenado T-SQL para importar en bloque, en SQL, los datos transformados

Los datos de cada almacén deben importarse por separado.

Copie el archivo `<StoreName>SQL.txt` creado en el paso 1 desde el escritorio del servidor de StoreFront en `C:\`, en el servidor Microsoft SQL, y cambie el nombre a SubscriptionsSQL.txt.

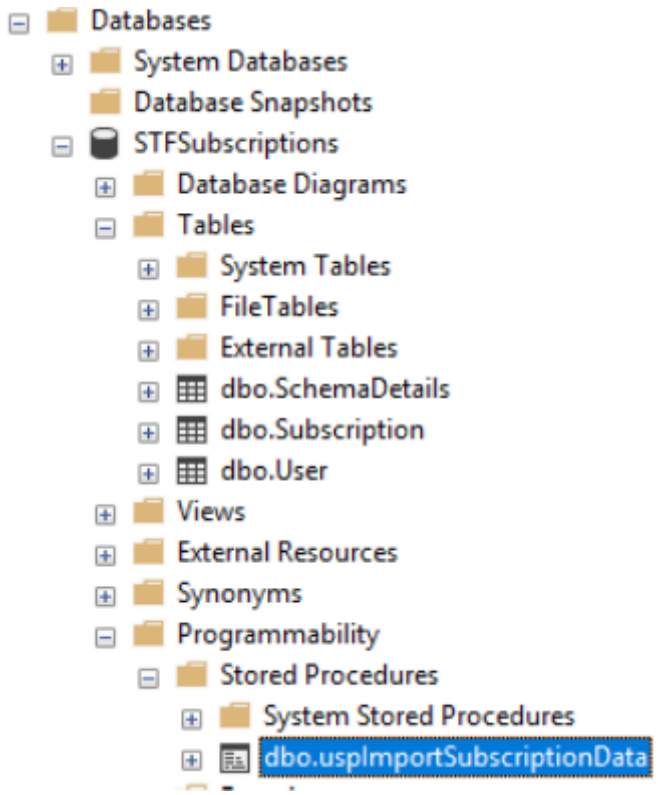
El script Create-importSubscriptionDataSP.sql crea un procedimiento almacenado T-SQL para importar los datos de suscripción en bloque. Además, elimina las entradas duplicadas para cada usuario único, de modo que los datos SQL resultantes se normalizan correctamente y se reparten en las tablas correctas.

Antes de ejecutar *Create-ImportSubscriptionDataSP.sql*, cambie `USE [STFSubscriptions]` para que coincida con la base de datos en la que quiere crear el procedimiento almacenado.

Abra el archivo *Create-ImportSubscriptionDataSP.sql* con SQL Server Management Studio y ejecute el código que contiene. Este script agrega el procedimiento almacenado *ImportSubscriptionDataSP* a la base de datos creada anteriormente.

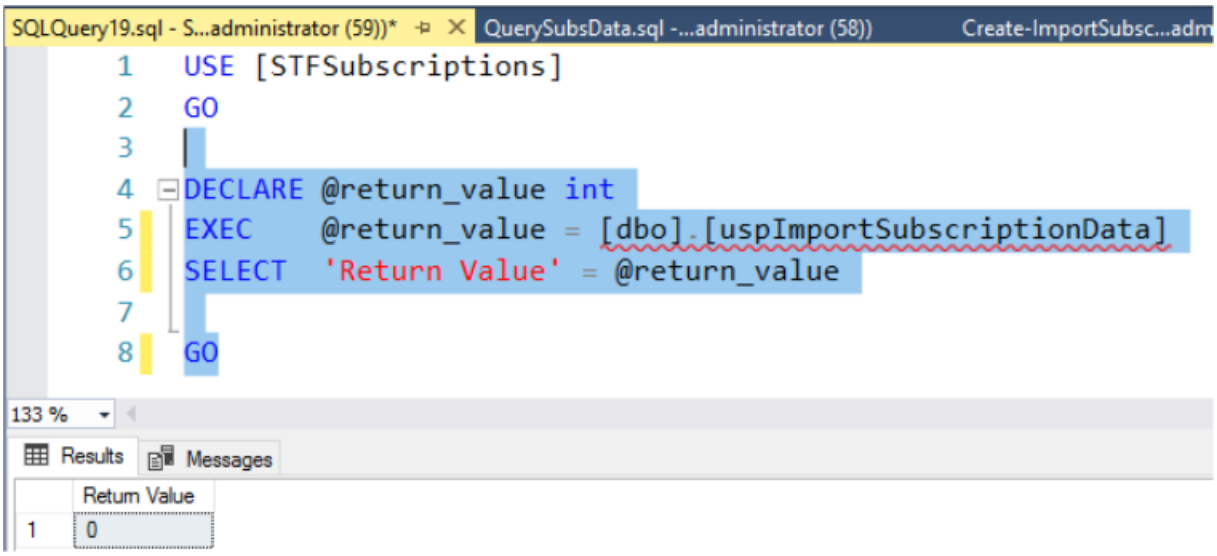
Después de crearse el procedimiento almacenado, se muestra el siguiente mensaje en la consola de SQL y se agrega el procedimiento almacenado ImportSubscriptionDataSP a la base de datos:

```
Commands completed successfully.
```



Para ejecutar el procedimiento almacenado, haga clic con el botón derecho en él, seleccione **Ejecutar**

procedimiento almacenado y haga clic en **Aceptar**.



El valor devuelto 0 indica que todos los datos se han importado correctamente. Cualquier problema al importar se registra en la consola de SQL. Una vez que el procedimiento almacenado se haya ejecutado correctamente, compare el número total de registros de suscripción y usuarios únicos que proporciona Transform-SubscriptionDataForStore.ps1 con el resultado de las dos consultas SQL siguientes. Los dos totales deben coincidir.

El número total de suscripciones del script de transformación debe coincidir con el número total notificado desde SQL por

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

El número de usos únicos del script de transformación debe coincidir con el número de registros de la tabla de usuario notificados desde SQL por

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

Si el script de transformación muestra 100 usuarios únicos y 1000 registros de suscripción totales, SQL debe mostrar los mismos dos números después de la migración.

Inicie sesión en StoreFront para comprobar si los usuarios existentes pueden ver sus datos de suscripción. Los registros de suscripción se actualizan en SQL cuando los usuarios suscriben o cancelan la suscripción de sus recursos. Los nuevos usuarios y los registros de suscripción también se crean en SQL.

Paso 3. Ejecute consultas T-SQL en los datos importados

> **Nota:**
>
> Todos los nombres de Delivery Controller distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente con las mayúsculas y minúsculas utilizadas en StoreFront.

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

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

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

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

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

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

Actualizar o eliminar registros de suscripción existentes mediante T-SQL

> **RENUNCIA DE RESPONSABILIDADES:**
>
> Todas las instrucciones SQL para actualización y eliminación de ejemplo las utiliza bajo su propio riesgo. Citrix no se hace responsable de ninguna pérdida o alteración accidental de sus datos de suscripción por el uso incorrecto de los ejemplos proporcionados. Las siguientes instrucciones T-SQL se proporcionan como guía para posibilitar una actualización sencilla. Haga una copia de seguridad de todos los datos de suscripción presentes en su base de datos SQL antes de intentar actualizar sus suscripciones o eliminar registros obsoletos. Si no se realizan las copias de seguridad necesarias, se pueden producir pérdidas o daños en los datos. Antes de ejecutar sus propias instrucciones UPDATE o DELETE de T-SQL en la base de datos de producción, pruebe con datos ficticios o con una copia redundante de los datos, fuera del entorno de la base de datos de producción real.
>
> **Nota:**
>
> Todos los nombres de Delivery Controller distinguen entre mayúsculas y minúsculas, y deben coincidir exactamente con las mayúsculas y minúsculas utilizadas en StoreFront.

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

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

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

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

```



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

-- Delete all subscription records for an application published via a specific delivery controller
Use [STFSubscriptions]
DELETE FROM [Subscription]
FROM [Subscription]
WHERE [resource_id] = 'DeliveryController.Application'
```

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

Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
```

```
-- Delete ALL subscription data from a particular database and reset the primary key clustered index to start numbering from 0.
-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
-- Can be useful whilst debugging data import issues to start with a clean database.

Use [STFSubscriptions]
DELETE FROM [Subscription]
DBCC CHECKIDENT ([Subscription], RESEED, 0)
DELETE FROM [User]
DBCC CHECKIDENT ([User], RESEED, 0)
```

Parámetros avanzados de los almacenes

January 31, 2020

Puede configurar propiedades avanzadas de los almacenes mediante la página Parámetros avanzados en Configurar parámetros del almacén.

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

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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione un almacén en el panel central y, a continuación, seleccione **Configurar parámetros del almacén**.
3. En la página **Configurar parámetros de almacén**, seleccione **Parámetros avanzados**, seleccione la opción que quiere configurar, haga el cambio necesario, y haga clic en **Aceptar**.

Tipo de resolución de direcciones

Utilice la página **Parámetros avanzados** para especificar el tipo de dirección que se debe solicitar desde el servidor. El valor predeterminado es DnsPort. Desde el menú desplegable **Tipo de resolución de direcciones** en **Ajustes avanzados**, seleccione uno de los siguientes:

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

Permitir suavizado de fuentes

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

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 quiere que las sesiones HDX puedan reconectarse. El valor predeterminado es Sí.

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

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 realiza comprobaciones de estado periódicas en cada uno de los brokers de Citrix Virtual Desktops y servidores Citrix Virtual Apps 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 un almacén 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** y especifique los segundos de espera que han de transcurrir al establecer la conexión inicial, y luego haga clic en **Aceptar**.

Habilitar enumeración mejorada

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

Utilice la tarea **Parámetros avanzados**, marque (o desmarque) la casilla **Habilitar enumeración mejorada**, y haga clic en **Aceptar**.

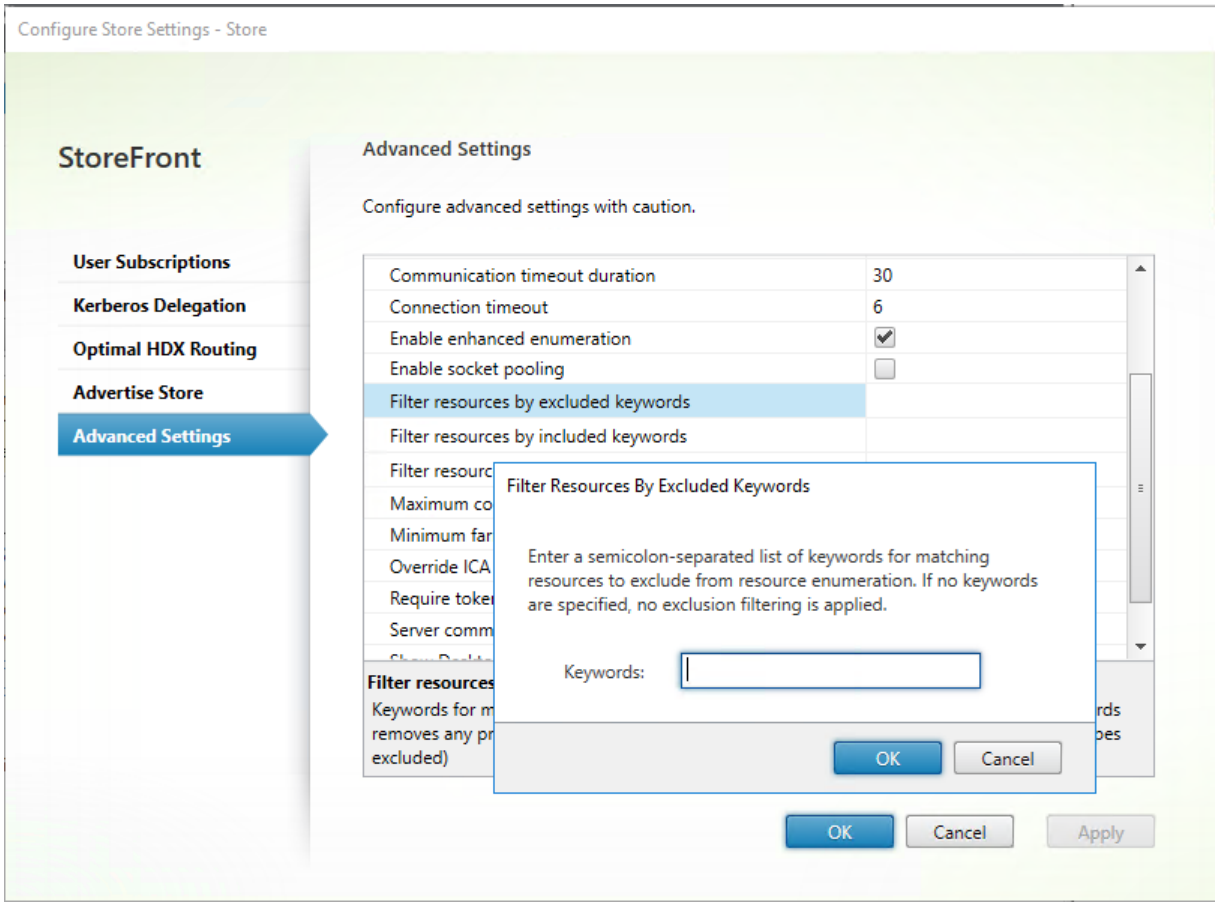
Habilitar la agrupación de sockets

De forma predeterminada, la agrupación de sockets está inhabilitada en los almacenes. 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, modifique el archivo de configuración del almacén. 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, la aplicación Citrix Workspace especifica el nombre del cliente. El valor predeterminado es No.

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 al almacén. Si los valores no son coherentes, los usuarios deben volver a autenticarse. Es necesario habilitar esta opción para aplicar SmartAccess. El valor predeterminado es Sí.

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 quiere 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 No.

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

Administrar un sitio de Citrix Receiver para Web

January 6, 2020

Un sitio de *Citrix Receiver para Web* es un sitio web que se utiliza como almacén de aplicaciones. Los usuarios pueden abrir el sitio en un explorador web y acceder de forma segura a las aplicaciones, los datos y los escritorios publicados para ellos a través de Citrix Virtual Apps and Desktops.

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

Tarea	Detalles
Crear un sitio de Citrix Receiver para Web	Cree sitios de Receiver para Web, que permiten a los usuarios acceder a almacenes a través de una página web.
Configurar sitios de Citrix Receiver para web	Modifique la configuración de los sitios de Receiver para Web.
Experiencia de usuario unificada	StoreFront ofrece la experiencia de usuario unificada. La experiencia unificada ofrece una experiencia de usuario en HTML5 que se puede administrar de forma centralizada.
Crear y administrar aplicaciones destacadas	Cree grupos de aplicaciones destacadas de productos, relacionadas o pertenecientes a una categoría específica, para los usuarios finales.
Configurar el 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.

Tarea	Detalles
Configurar el uso de fichas del explorador web con la aplicación Citrix Workspace para HTML5	Cuando los usuarios inician recursos con Citrix Receiver para HTML5 o la aplicación Citrix Workspace para HTML5 a partir de accesos directos, especifique si el escritorio o la aplicación reemplazan el sitio de Citrix Receiver para Web en la ficha existente del explorador en vez de aparecer en una nueva ficha.
Configurar la duración del tiempo de espera en las comunicaciones y los reintentos	De forma predeterminada, el tiempo de espera de las solicitudes de un sitio de Citrix Receiver para Web para el almacén asociado se agota pasados tres minutos. El almacén se considera no disponible después de un intento de comunicación fallido. Si quiere, puede cambiar el parámetro predeterminado.

Crear un sitio de Citrix Receiver para Web

January 31, 2020

Al crear un almacén, se crea automáticamente un sitio de Citrix Receiver para Web vinculado a él. Puede agregar sitios adicionales de Citrix Receiver para Web a los almacenes existentes.

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

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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione el almacén 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. Escriba la **ruta del sitio web** correspondiente y haga clic en **Siguiente** .
4. Seleccione la experiencia de Citrix Receiver y haga clic en **Siguiente**.
5. Seleccione Métodos de autenticación, haga clic en **Crear** y, cuando se haya creado el 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 la modificación de parámetros de sitios de Citrix Receiver para Web, consulte Configurar 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 la aplicación Citrix Workspace está instalada en el dispositivo de usuario. Si no se detecta la aplicación Citrix Workspace, se solicita al usuario que la descargue del sitio web de Citrix y la instale en su plataforma. Para obtener más información sobre cómo modificar este comportamiento, consulte Configurar el comportamiento del sitio para los usuarios sin la aplicación Citrix Workspace.

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

Configurar sitios de Citrix Receiver para web

March 2, 2020

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 Configurar 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado,
> propague los cambios de configuración al grupo de servidores para que se actualicen los demás

> servidores de la implementación.

Elegir los métodos de autenticación

Utilice la tarea Administrar 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 **Almacén** en el panel izquierdo de la consola de administración de Citrix StoreFront. A continuación, seleccione el almacén que quiera modificar en el panel Almacenes.
3. En el panel Almacenes, 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 **Nombre de usuario y contraseña** para habilitar la autenticación explícita. Los usuarios introducen sus credenciales cuando acceden a sus almacenes.
    - Seleccione **Autenticación SAML** para permitir la integración en proveedores de identidades SAML. Los usuarios se autentican en un proveedor de identidades y su sesión se inicia automáticamente cuando acceden a sus almacenes. Desde el menú desplegable Parámetros:
        - Seleccione **Proveedor de identidades** para configurar la confianza en 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 los almacenes. Para poder usar esta opción, la autenticación PassThrough debe estar habilitada cuando se instalan Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows en los dispositivos de los usuarios.

      > Nota:
      >
      > La autenticación PassThrough de dominios en Citrix Receiver para Web está limitada a sistemas operativos Windows que utilicen Chrome, Firefox e Internet Explorer.

- Marque **Tarjeta inteligente** para habilitar la autenticación con tarjeta inteligente. Los usuarios realizan la autenticación con tarjetas inteligentes y PIN cuando acceden a los almacenes.
- Marque **PassThrough desde Citrix Gateway** para habilitar la autenticación PassThrough desde Citrix Gateway. Los usuarios se autentican en Citrix Gateway y su sesión se inicia automáticamente cuando acceden a sus almacenes.

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 Configurar el servicio de autenticación.

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 de confianza 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 vínculos 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.

Para poder generar accesos directos a recursos, debe agregar las direcciones URL de sitios web host a la lista "URL de confianza" desde la consola de administración de Citrix StoreFront o mediante PowerShell. Las direcciones URL de confianza se indican en la sección `<trustedUrls>` del archivo web.config del sitio de Citrix Receiver para Web. El archivo web.config suele encontrarse en el directorio `C:\inetpub\wwwroot\Citrix\storenameWeb\`, donde *storename* es el nombre especificado para el almacén cuando se creó.

De forma predeterminada, StoreFront avisa a los usuarios si intentan iniciar accesos directos a recursos desde sitios web que no son de confianza, pero los usuarios pueden optar por iniciar el recurso igualmente. Para que esos avisos dejen de aparecer, en el panel Almacenes, haga clic en **Administrar sitios de Receiver para Web**, haga clic en **Configurar**, elija **Parámetros avanzados** y desactive la opción **Preguntar si no se confía en los accesos directos**.

Agregar sitios web de confianza desde la consola de administración

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 **Almacenes** 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**, 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 siguiendo 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 quiere 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 que se requieren al sitio web.

Agregar sitios web de confianza mediante PowerShell

Puede agregar direcciones URL "de confianza" mediante el cmdlet de PowerShell **Set-STFWebReceiverApplicatior** descrito en https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Citrix.StoreFront.SubscriptionsStore/.

Definir el 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 **Almacenes** 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.

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 **Almacenes** 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 **Almacenes** 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**.

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 o la aplicación Citrix Workspace para el almacén asociado. Los archivos de aprovisionamiento contienen los datos de conexión para el almacén que proporciona los recursos en el sitio, incluidos los detalles de las implementaciones de Citrix Gateway y las balizas configuradas para el almacén. En este artículo, las menciones de “aplicación Citrix Workspace” también representan las versiones compatibles de Citrix Receiver, a menos que se indique lo contrario.

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 **Almacenes** 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 la aplicación Workspace/Receiver**.

Configurar el comportamiento del sitio para los usuarios sin la aplicación Citrix Workspace

Utilice la tarea **Implemente la aplicación Workspace/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 la aplicación Citrix Workspace acceda al sitio. De forma predeterminada, los sitios de Citrix Receiver para Web intentan detectar automáticamente si la aplicación Citrix Workspace está instalado cuando se accede a ellos desde equipos con Windows o Mac OS X.

Si no se detecta la aplicación Citrix Workspace, se solicita al usuario que la descargue y la instale para su plataforma. La ubicación de descarga predeterminada es el sitio web de Citrix, pero también puede copiar los instaladores de la aplicación Citrix Workspace en el servidor de StoreFront y permitir a los usuarios descargar copias de estos directamente desde el servidor de StoreFront.

Para los usuarios que no pueden instalar la aplicación Citrix Workspace, puede habilitar la aplicación Citrix Workspace para HTML5 en los sitios de Citrix Receiver para Web. La aplicación Citrix Workspace para HTML5 permite a los usuarios acceder a escritorios y aplicaciones directamente desde exploradores web compatibles con HTML5 sin necesidad de instalar la aplicación Citrix Workspace. Se admiten tanto las conexiones internas de red como las conexiones a través de Citrix Gateway. Sin embargo, si se trata de conexiones desde la red interna, la aplicación Citrix Workspace para HTML5 solo permite el acceso a los recursos proporcionados por productos específicos. Además, se necesitan versiones específicas de Citrix 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 la aplicación Citrix Workspace para HTML5 para los recursos proporcionados por Citrix Virtual Apps and Desktops se encuentra inhabilitado para los usuarios locales de la red interna. Para habilitar el acceso local a escritorios y aplicaciones mediante la aplicación Citrix Workspace para HTML5, debe habilitar la directiva Conexiones de WebSockets en los servidores Citrix Virtual Apps and Desktops. Citrix Virtual Apps and Desktops utiliza el puerto 8008 en las conexiones de la aplicación Citrix Workspace 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.

Para que el recurso de Citrix Virtual Apps and Desktops se inicie correctamente con la aplicación Citrix Workspace para HTML5 al conectarse directamente a StoreFront, deben configurarse las conexiones TLS a los VDA que alojan aplicaciones y escritorios. Las conexiones remotas a través de Citrix Gateway pueden iniciar recursos mediante la aplicación Citrix Workspace para HTML5 sin configurar conexiones TLS al VDA.

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 **Almacén** 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 la aplicación Workspace/Citrix Receiver** y especifique una **opción de implementación**.
    - Seleccione **Usar siempre Receiver para HTML5** si quiere que el sitio siempre acceda a los recursos a través de un explorador compatible con HTML5 sin pedir al usuario que descargue e instale la aplicación Citrix Workspace. Con esta opción seleccionada, los usuarios siempre acceden a escritorios y aplicaciones del sitio a través de la aplicación Citrix Workspace para HTML5, siempre que utilicen un explorador compatible con HTML5. Los usuarios sin un explorador compatible con HTML5 no pueden acceder a los recursos. El acceso a través de cualquier aplicación Citrix Workspace instalada localmente está inhabilitado.
    - Seleccione **Usar Receiver para HTML5 si el Receiver local no está disponible** si quiere que el sitio solicite al usuario que descargue e instale la aplicación Citrix Workspace pero que recurra a la aplicación Citrix Workspace para HTML5 si la aplicación Citrix Workspace no puede instalarse. A los usuarios sin la aplicación Citrix Workspace se les solicitará que la descarguen y la instalen cada vez que inicien sesión en el sitio.
    - Seleccione **Instalar localmente** si quiere que el sitio siempre tenga acceso a los recursos a través de una aplicación Citrix Workspace instalada localmente. Se solicita a los usuarios que descarguen e instalen la aplicación Citrix Workspace adecuada para su plataforma. El acceso a través de exploradores compatibles con HTML5 está inhabilitado.
        - Si selecciona **Permitir que los usuarios descarguen el plug-in de HDX Engine**, Citrix Receiver para Web permite que el usuario descargue e instale la aplicación Citrix Workspace en el cliente del usuario final si la aplicación Citrix Workspace no está disponible en él.
        - Si selecciona **Actualizar el plug-in al iniciar sesión**, Citrix Receiver para Web ofrece a los usuarios la opción de actualizar el cliente de la aplicación Citrix Workspace cuando inician sesión. Los usuarios pueden optar por omitir la actualización y no se les ofrecerá esta actualización a menos que se borren las cookies del explorador de Citrix Receiver para Web. Para habilitar esta función, asegúrese de que los archivos de la aplicación Citrix Workspace están disponibles en el servidor de StoreFront.
        - Seleccione un origen de archivos en la lista desplegable.

Ofrecer los archivos de instalación de la aplicación Citrix Workspace 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 la aplicación Citrix Workspace está instalada en el dispositivo de usuario. Si no se puede detectar la aplicación, se le pedirá al usuario que la descargue desde el sitio web de Citrix y la instale en su plataforma o que descargue el instalador correcto desde el servidor 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 **Almacén** 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 la aplicación Workspace/Citrix Receiver** y **Archivos de origen para la aplicación Workspace/Receiver** y, a continuación, busque los archivos de instalación.

Mostrar la solicitud para instalar la aplicación Citrix Workspace después de iniciar sesión

Antes de iniciar sesión en StoreFront, Citrix Receiver para Web solicita al usuario que instale la aplicación de Citrix Workspace más reciente si aún no está instalada en el equipo del usuario. Según la configuración, el mensaje también puede indicar si la instalación de la aplicación Citrix Workspace 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 **Almacenes** 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 la aplicación Workspace/Receiver después de iniciar la sesión**.

Eliminar 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 al almacén.

Experiencia de usuario unificada

March 2, 2020

> Nota:
>
> El término “StoreFront” sigue siendo el nombre utilizado para referirse a un almacén de aplicaciones de empresa que combina aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops en un único e intuitivo almacén para los usuarios. Ahora, la tecnología de Citrix Receiver está incluida en la aplicación Citrix Workspace. La implementación de esta transición en nuestros productos y documentación es un proceso continuo. El contenido del producto aún puede contener nombres anteriores; por ejemplo, la experiencia unificada se conoce como “Citrix Receiver” en el producto. Agradecemos su comprensión durante esta transición. Para obtener más información detallada sobre nuestros nuevos nombres, consulte https://www.citrix.com/about/citrix-product-guide/.

StoreFront ofrece la experiencia de usuario *unificada*. La experiencia unificada ofrece una experiencia de usuario en HTML5 administrada de forma centralizada para todas las aplicaciones web y nativas Citrix Workspace. Se admite la personalización y la administración de grupos de aplicaciones destacadas.

Los almacenes creados con esta versión de StoreFront emplean la experiencia unificada.

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 al almacén.
- Personalizar la apariencia de Receiver.

Use JavaScript y CSS para personalizar las páginas de Citrix Receiver para Web.

En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás 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, las aplicaciones configuradas para **Distribuir al cliente** o **Distribuir si es posible, de lo contrario se accede desde un servidor** no se admiten en la experiencia unificada habilitada.

Crear un sitio web de Citrix Receiver para Web

Cada vez que se crea un almacén, 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 Almacenes 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.

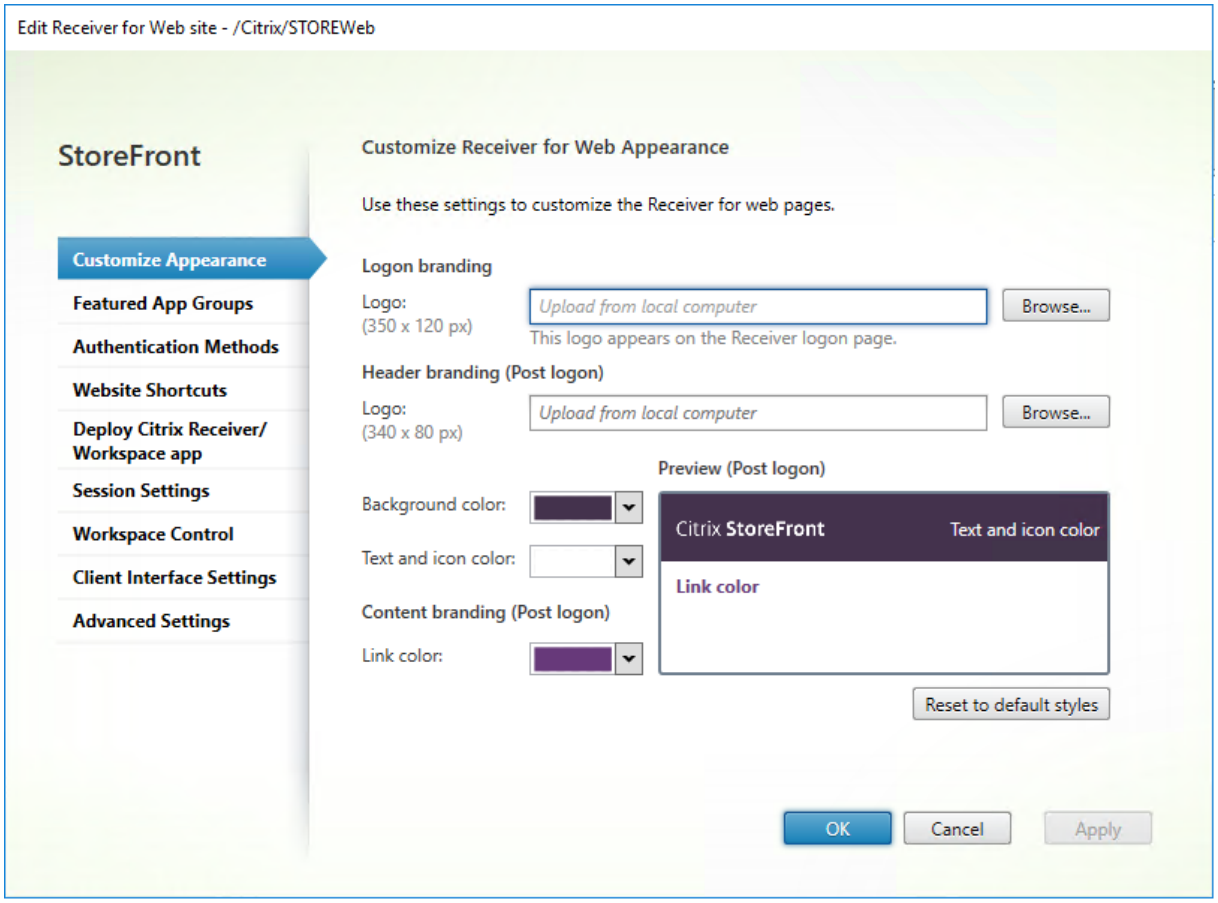
Seleccionar un sitio de Citrix Receiver para Web para asociarlo al almacén

Cuando se crea un almacén mediante StoreFront, también se crea automáticamente un sitio de Citrix Receiver para Web y se asocia a dicho almacén. Los sitios de Citrix Receiver para Web emplean la experiencia unificada. Cuando un almacén tiene varios sitios de Receiver para Web, debe seleccionar qué sitio de Receiver para Web se muestra cuando los usuarios acceden al almacén mediante la aplicación Citrix Workspace.

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 **Almacén** en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione un almacén en el panel central y, a continuación, seleccione **Configurar la experiencia unificada** en el panel **Acciones**. Si no dispone de un sitio web creado de Citrix Receiver para Web, aparecerá un mensaje con un enlace al asistente para agregar un sitio de Receiver para Web.
3. Seleccione el sitio predeterminado de Receiver para Web que los clientes de la aplicación Citrix Workspace muestran cuando los usuarios acceden a este almacén.
4. Haga clic en **Aceptar**.

Personalizar la apariencia de Citrix Receiver

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 **Almacenes** 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 en **Configurar**.
3. Seleccione **Personalizar apariencia** y realice las selecciones necesarias para personalizar cómo se muestra el sitio web después de iniciar sesión.



Personalización adicional mediante JavaScript y CSS

> Nota:
>
> En los ejemplos de esta sección, agregue JavaScript al archivo *script.js* (por ejemplo, en C:\inetpub\wwwroot\Citrix\StoreWeb\Custom) y agregue CSS al archivo *style.css* en el mismo directorio.

Agregar un encabezado estático a la página de inicio de sesión en Receiver para Web

Aquí, "estático" se refiere a un texto fijo, como un mensaje de bienvenida o el nombre de una empresa. Para mostrar algo que cambia, como noticias o mensajes sobre el estado del servidor, consulte Agregar un encabezado dinámico a la página de inicio de sesión en Receiver para Web.

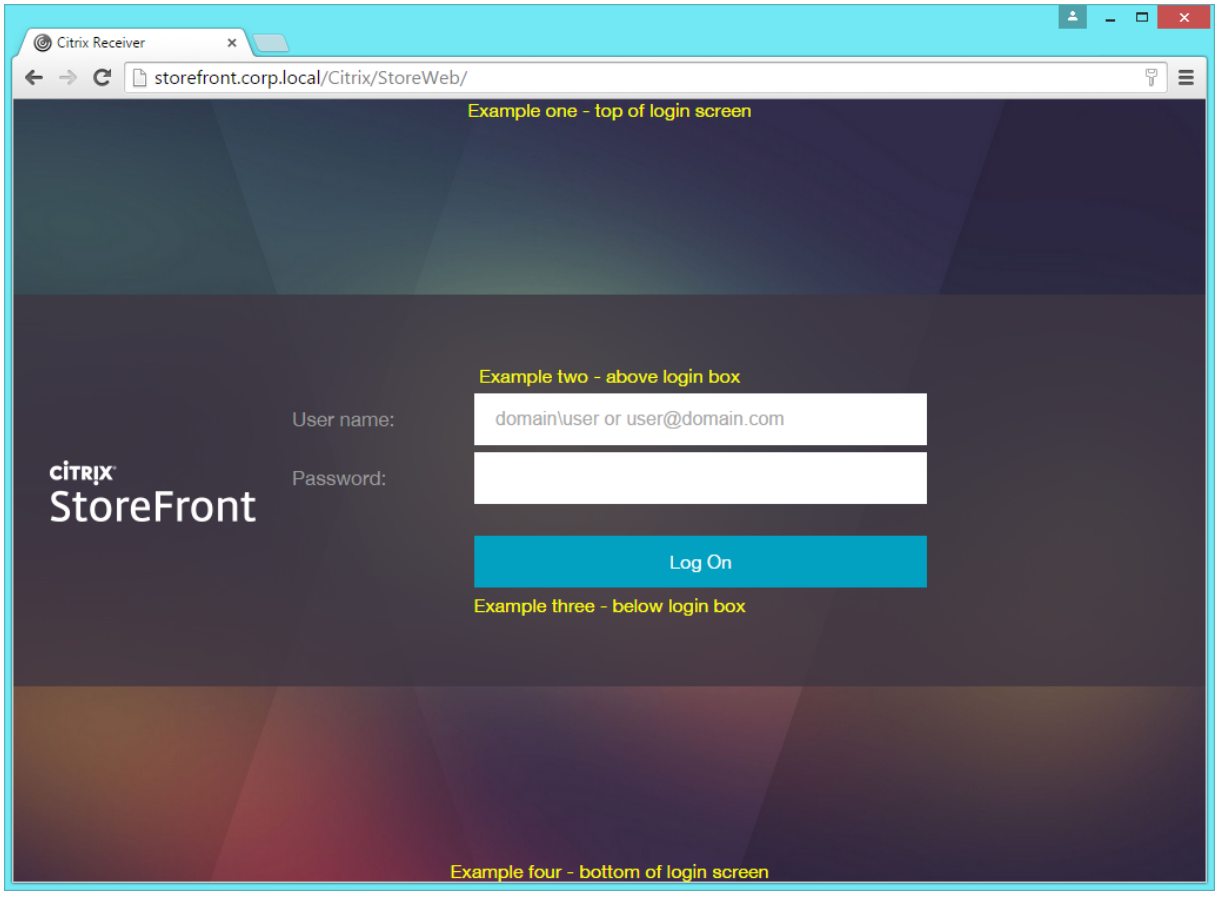
Puede agregar texto estático en cuatro posiciones mediante las siguientes líneas de JavaScript:

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


Para que el texto sea más visible, agregue el siguiente estilo a custom.css:

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

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

Esto da el siguiente resultado:



Para usar el formato HTML, reemplace las 4 líneas de JavaScript por lo siguiente:

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



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

> Nota:
>
> La cuarta línea del ejemplo espera una imagen llamada *logo.png* en el directorio personalizado.

Agregar un encabezado dinámico a la página de inicio de sesión en Receiver para Web

Aquí, "dinámico" se refiere a que parte del contenido se carga y se muestra cada vez, en lugar de almacenarse en caché. Los exploradores web suelen almacenar en caché las cosas cuando pueden, pero la aplicación Citrix Workspace siempre almacena en caché la interfaz de usuario y siempre carga la interfaz de usuario anteriormente almacenada en caché. Eso significa que, si usa el ejemplo anterior para algo así como el estado del servicio, no obtendrá lo que esperaba.

En su lugar, debe realizar una llamada Ajax para cargar de manera dinámica el contenido e insertarlo en la página. Para hacerlo:

1. Defina una función de utilidad práctica que obtenga el contenido de una página en el directorio *\customweb* del servidor y lo agregue a la página. Esto hace las veces de equivalente de los ejemplos HTML anteriores, y la página personalizada puede contener texto o un fragmento HTML. Utilice el directorio *\customweb* porque se copia en todos los servidores de un grupo de servidores de StoreFront (al igual que el directorio \custom), pero no se descarga ni se almacena en caché.
2. Haga que esta función se llame en el momento adecuado. Si se la llama demasiado pronto, provocará problemas en la aplicación Citrix Workspace, ya que el script se ejecuta antes de que la configuración se haya cargado por completo. Un buen momento para este tipo de acción es **beforeDisplayHomeScreen** (pero si quiere mostrar contenido en la página de inicio de sesión, utilice **beforeLogin** en su lugar). El siguiente código contempla los dos casos y es adecuado para clientes web y nativos.

El script completo es el siguiente:

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



```
  }
 );
 }


var fetchedContent=false;
function doFetchContent(callback)
{

  if(!fetchedContent) {

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

  callback();
 }


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

Esto carga contenido de *\customweb\readme.txt* que, de forma predeterminada, contiene información poco interesante. Agregue su propio archivo (*status.txt*) y modifique el script para llamarlo y, así, obtener resultados más útiles.

Mostrar una exención de responsabilidad por el que avanzar con clics antes o después de iniciar sesión

El siguiente ejemplo ya se proporciona en el archivo *script.js* como ejemplo, pero necesita quitarle las marcas de comentario. Hay dos versiones de este código: la primera se realiza antes del inicio de sesión para los exploradores web, y la segunda se realiza antes de mostrar la interfaz de usuario principal para los clientes nativos. Si solo quiere un mensaje posterior al inicio de sesión, elimine la primera función. Sin embargo, usar un mensaje antes del inicio de sesión por sí solo no es una buena opción, ya que el flujo de inicio de sesión solo se ve en exploradores web (y no en clientes nativos). Incluso entonces, el flujo de inicio de sesión se oculta cuando los usuarios acceden desde Citrix Gateway.

```
var doneClickThrough = false;

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

```



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

    messageTitle: "Welcome!",
    messageText: "Only for WWCo Employees",
    okButtonText: "Accept",
    okAction: callback
   }
);
}
;

// Before main screen (both web and native)
CTXS.Extensions.beforeDisplayHomeScreen = function (callback) {

  if (!doneClickThrough) {

    CTXS.ExtensionAPI.showMessage({

      messageTitle: "Welcome!",
      messageText: "Only for WWCo Employees",
      okButtonText: "Accept",
      okAction: callback
     }
);
  }
  else {

    callback();
  }

}
;
```

Ampliar el cuadro de exención de responsabilidad por el que avanzar con clics

El cuadro de mensaje utilizado para **CTXS.ExtensionAPI.showMessage()** está predefinido. Puede modificar este estilo para ampliar el cuadro, de modo que se muestre correctamente para otros mensajes. Agregue la siguiente función de ejemplo a script.js para volver a reducir el estilo más adelante. Llame a **showLargeMessage()** en lugar de **CTXS.ExtensionAPI.showMessage()** cuando quiera un cuadro más grande.

```
function mkLargeMessageExitFn(origfn)
```



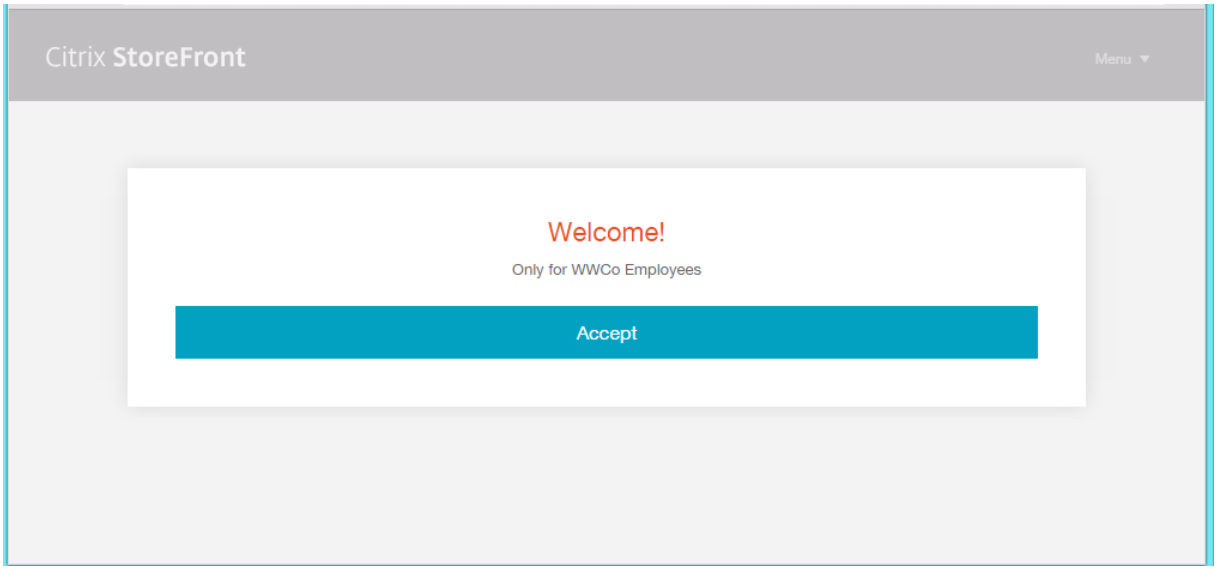
```
{

  if(origfn) {

    return function() {

      origfn();
      window.setTimeout(function() {
 $('body').removeClass('largeMessage'); }
 ,500);
     }
 ;
   }

 }


function showLargeMessage(details)
{

  $('body').addClass('largeMessage');
  details.cancelAction = mkLargeMessageExitFn(details.cancelAction);
  details.okAction = mkLargeMessageExitFn(details.okAction);
  CTXS.ExtensionAPI.showMessage(details);
 }
 ;
```

Esto agrega una clase de marcador cuando se muestra el mensaje grande. Al cerrar el cuadro, se elimina esta clase de marcador tras unos instantes (necesarios para evitar un "salto" desagradable).

Agregue un poco de CSS para ajustar el tamaño de este cuadro en función de la presencia de esta clase de marcador. Por ejemplo, pruebe lo siguiente en custom\style.css:

```
.largeTiles .largeMessage .messageBoxPopup
{

  width:800px;
 }
```

A continuación, cuando se muestra un elemento messageBoxPopup en una interfaz de usuario grande y se establece el indicador largeMessage, tiene 800 píxeles de ancho. El código existente garantiza que esté centrado (en una interfaz de usuario pequeña, como la de un teléfono móvil, el cuadro de mensaje predeterminado ya es de ancho completo).



Para meter aún más texto, puede reducir el tamaño de fuente; para ello, agregue lo siguiente a custom\style.css o, si no, también puede agregar contenido por el que se pueda desplazar.

```
.largeTiles .largeMessage .messageBoxText
{

  font-size:10px;
 }
```

Hacer que el cuadro de exención de responsabilidad por el que avanzar con clics tenga contenido por el que se pueda desplazar

Al llamar a **showMessage**, puede agregar algo de HTML (en lugar de solo una cadena) para agregar estilo. Para ello, en cualquiera de las llamadas de ejemplo anteriores a showMessage, reemplace messageText por lo siguiente:

```
    CTXS.ExtensionAPI.showMessage({

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

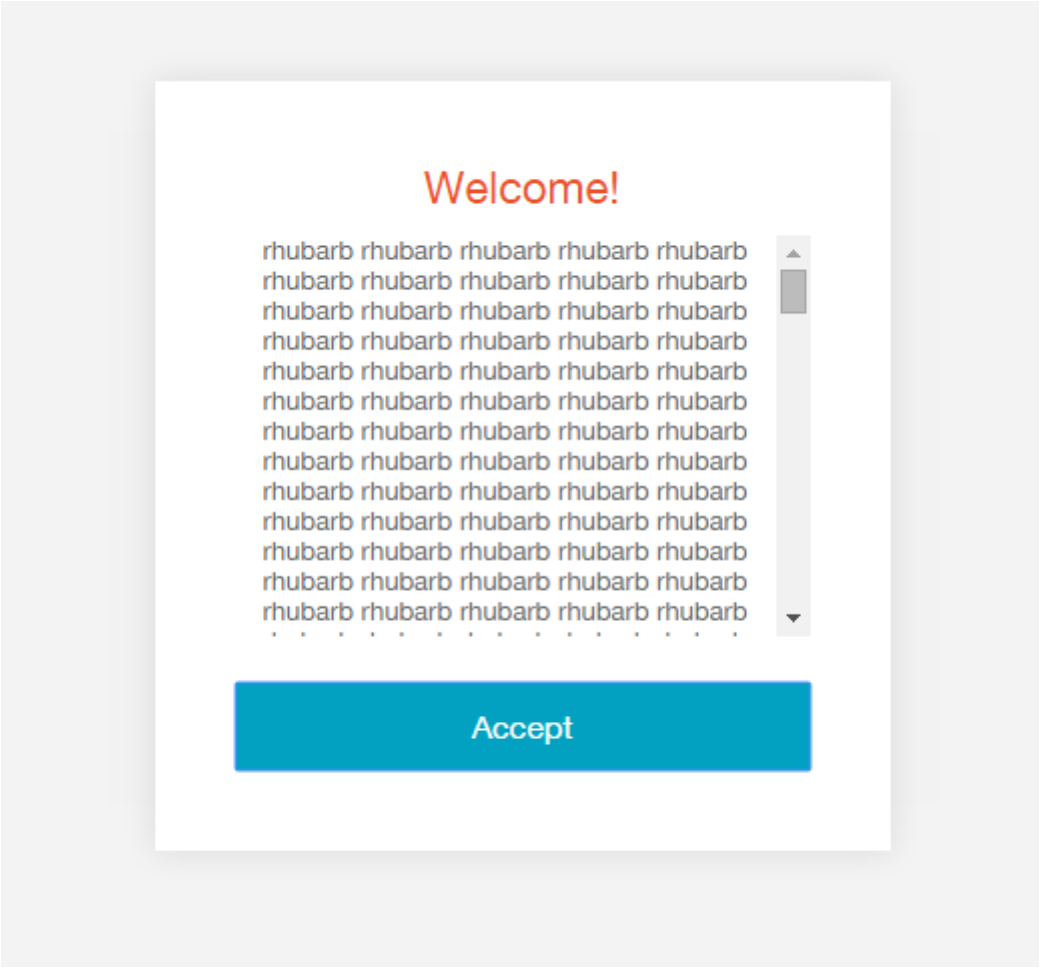
A continuación, agregue lo siguiente a style.css:

```
.disclaimer {
```



```
2
3       height: 200px;
4       overflow-y: auto;
5   }
```

Esto da el siguiente resultado:



Agregar un pie de página a cada página

Hay otra área personalizada específicamente para esto. Puede agregar la siguiente línea de JavaScript para establecer su contenido:

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

Defina el estilo en style.css. Establezca `position:static` para cerciorarse de que el área de desplazamiento funciona como se espera.

```
1  #customBottom
```



```
{

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

> Nota:
>
> Si cambia de tamaño dinámicamente esta área mediante un script, debe llamar al comando **CTXS.ExtensionAPI.resize()** para que la aplicación Citrix Workspace sepa que algo ha cambiado.

Convertir la vista de carpetas en predeterminada cuando los usuarios vayan a la ficha Aplicaciones

Para ello, supervise el evento "cambio de vista". Si cambia la vista al "almacén" (el nombre interno de la vista de aplicaciones), vaya a la carpeta raíz. Cuidado con lo siguiente:

- Cuando se activa el evento **onViewChange**, para decir que la vista de almacén va a cambiar, la vista no ha terminado de representarse en la pantalla. Por lo tanto, si va a la carpeta inmediatamente, el código de inicialización de la vista de almacén simplemente deshará su trabajo, ya que se ejecuta después del código. Para evitar esto, agregue un retraso de 1 ms para asegurarse de que el código se ejecuta después de que la pila actual se desenrede.
- Las tres líneas que contienen la palabra "whitespace" aseguran que la interfaz de usuario inicial de Todas las aplicaciones se represente fuera de la pantalla mediante una gran área personalizada que se coloca encima de ella. Esto detiene el parpadeo de la vista de Todas las aplicaciones antes de que aparezcan las carpetas.

Agregue el siguiente código a script.js como de costumbre:

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

CTXS.Extensions.onViewChange = function(view) {

  if (view == "store") {

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

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



```
      }
  , 1);
    }

}
;
```

Ocultar aplicaciones de Todas las aplicaciones que también aparecen en una categoría destacada

Puede usar el siguiente código para lograr esto. Empiece por recordar todas las aplicaciones de un paquete y, a continuación, quítelas de la lista “All Apps display”.

```
var bundleApps = [];

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

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

    bundleApps.push(apps[i]);
   }

  defaultfn();
 }
 ;

CTXS.Extensions.filterAllAppsDisplay = function(allapps) {

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

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

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

   }

}
;
```

Si utiliza esta personalización, es buena idea cambiar la cadena de texto “All Apps” por “Other Apps” para evitar que los usuarios se confundan. Para ello, modifique el archivo *strings.en.js* en el directo-

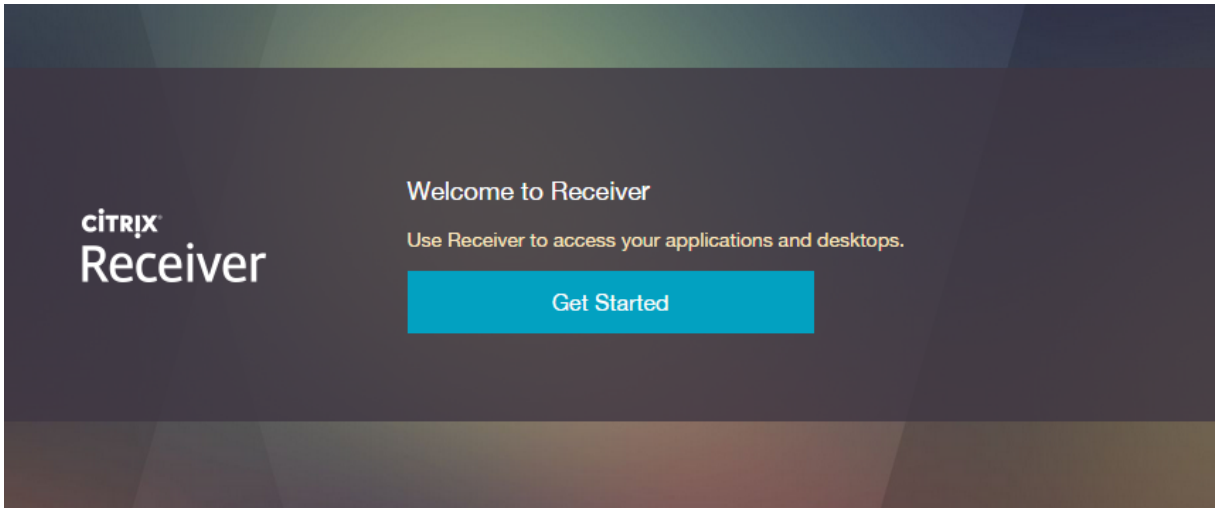
rio personalizado y, luego, agregue una etiqueta para **AllAppsTitle**. Por ejemplo, con los siguientes cambios en amarillo:

```
(function ($) {

  $.localization.customStringBundle(”en”, {

   <span style=”background-color: yellow;”>AllAppsTitle: ”Other Apps”
      ,</span>
   Example1: ”This is an example”,
   Example2: ”This is another example”
 }
 );
 }
 )(jQuery);
```

Cambiar el texto predeterminado de la interfaz de usuario

Puede cambiar el texto utilizado en la interfaz de usuario si sabe cómo se llama la etiqueta correspondiente. Por ejemplo, para cambiar la pantalla “Install” utilizada en Receiver para Web en Google Chrome por “Get Started”, agregue una cadena personalizada de la siguiente manera:

```
(function ($) {

  $.localization.customStringBundle(”en”, {

   <span style=”background-color: yellow;”>Install: ”Get Started”,</
      span>
   Example1: ”This is an example”,
   Example2: ”This is another example”
 }
 );
 }
 )(jQuery);
```

Para descubrir el nombre de la etiqueta que quiere cambiar:

1. En el servidor de StoreFront, busque en el directorio C:\inetpub\wwwroot\citrix\StoreWeb\receiver\js\localiz (asumiendo que su almacén se llama “Store”).
2. Abra el archivo *ctxs.strings_algo.js* en el Bloc de notas.
3. Busque la cadena que quiera cambiar. **Nota**: En lugar de modificar este archivo directamente, cree valores de reemplazo en el directorio personalizado como en el ejemplo de “install”.

Cambiar las imágenes de fondo de las categorías destacadas

> Importante:
>
> No intente sobrescribir las imágenes en el servidor. Esto confunde a los clientes que ya han descargado las imágenes porque no saben que han cambiado. También hace que la actualización resulte difícil o imposible.

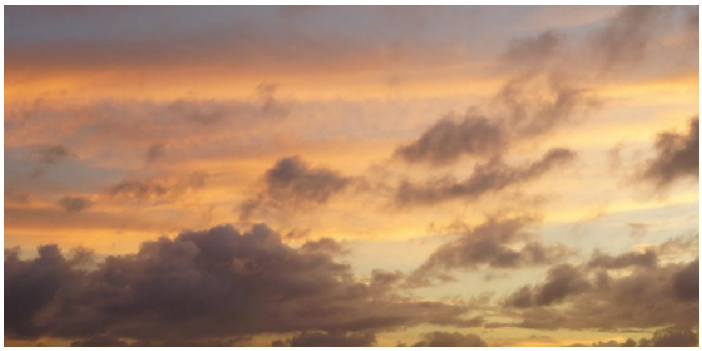
Puede agregar sus propias imágenes al directorio *custom* y agregar CSS para hacer referencia a ellas. Cada categoría destacada (llamada “bundle” o “paquete” internamente) utiliza dos imágenes:

- La primera imagen se usa como un icono en el carrusel.
- La segunda imagen se utiliza como imagen de fondo en el encabezado de la página de detalles. Esta imagen se estira para ocupar el ancho de la pantalla, y se agrega un efecto de desenfoque en el borde inferior.

Puede utilizar imágenes diferentes para cada pantalla. Piense en utilizar la misma imagen pero duplicando su altura de fondo en la página de detalles, de modo que solo se muestre la mitad superior de la imagen. Como la imagen se estira en la página de detalles, utilice una imagen que se vea bien si se deforma.

El primer paquete tiene la clase “appBundle1”, el segundo, “appBundle2”, y así sucesivamente hasta “appBundle8”. El siguiente ejemplo utiliza la imagen “clouds.png”, que puede descargar si hace clic

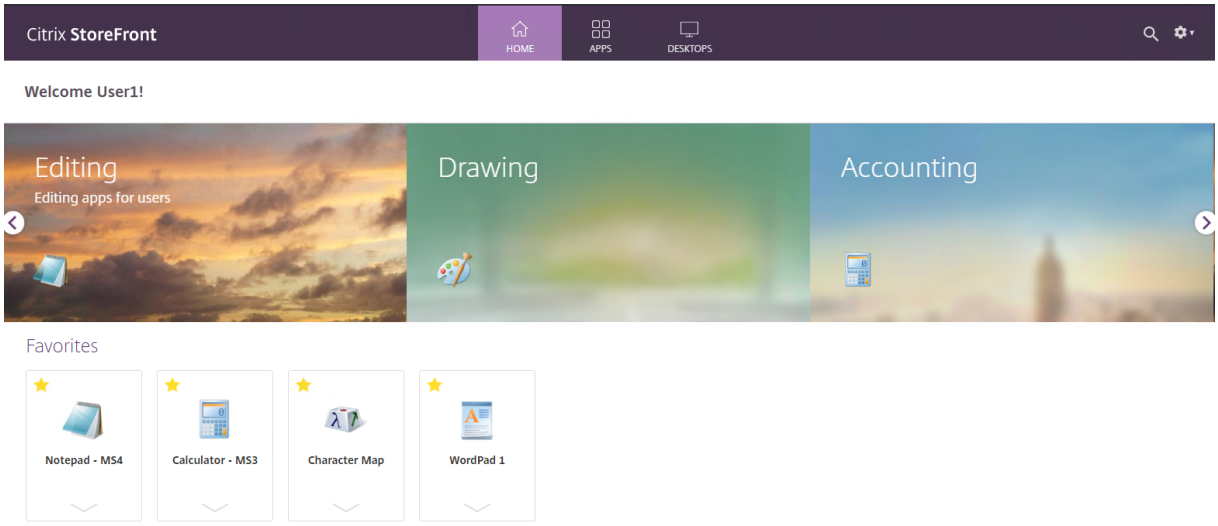
con el botón secundario en esta imagen:

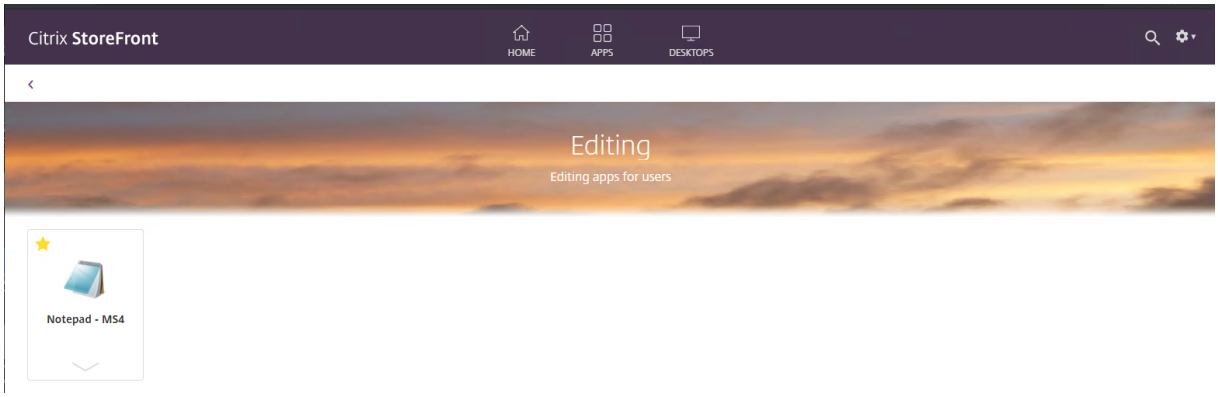


1. Guarde la imagen en el directorio *custom*. El tamaño de la imagen debe ser de unos 520×256 píxeles para ser coherente con las demás (pero se escala si es necesario).
2. Agregue esto a style.css:

```
.appBundle1 {

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


.bundleDetail.appBundle1 {

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

Esto da el siguiente resultado:





Evitar que el logotipo de una empresa se vea borroso

Receiver para Web necesita gestionar correctamente tanto las pantallas normales (“nivel bajo de ppp”) como las pantallas de alta resolución (“nivel alto de ppp”) más nuevas que tengan un mayor número de píxeles por pulgada cuadrada. Por ejemplo, las pantallas Retina de Apple tienen el doble de resolución que las pantallas que no son Retina. En los portátiles, las pantallas suelen tener 1,5, 2 o incluso 3 veces el número “normal” de píxeles para su tamaño. Como 2 veces (x2) es, de lejos, el caso más común y es donde se nota más la diferencia, la aplicación Citrix Workspace tiene la mayoría de sus recursos de imagen en dos resoluciones. Las imágenes con un tamaño de 100×100 píxeles en una pantalla normal también tienen una versión x2 a 200×200 píxeles.

Al cargar logotipos desde la consola de administración de StoreFront, las imágenes deben ser del tipo x2. Es decir, que son aproximadamente el doble de ancho y de altura del “espacio” de una pantalla normal (las imágenes cargadas en x1 no se amplían a x2). El “espacio” en una pantalla normal es de 170×40 píxeles, por lo que la imagen del logotipo que cargue debe ser de 340×80 píxeles aproximadamente.

StoreFront crea una copia del logotipo y lo escala a la mitad de su tamaño. Esta imagen se utiliza en pantallas con un nivel bajo de ppp.

A veces, esto da como resultado una imagen borrosa porque el detalle de la mitad de la imagen se ha descartado. Esto no es común, ya que los logotipos suelen ser llamativos y simples. Si su logotipo sufre este problema, utilice la siguiente solución:

1. Cree dos versiones de su logotipo, una en el tamaño x1 y otra en el tamaño x2, y guárdelas en el directorio *\custom*.
2. Modifique *custom\style.css* para que haga referencia a las dos imágenes. El resultado es similar a esto:

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



```
<span style="color: green;">/\* CITRIX DISCLAIMER: END OF MANAGED SECTION. \*/</span>
<span style="color: green;">/\* You may add custom styles below this line. */</span>

.logo-container {

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


.highdpi .logo-container {

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

> Nota:
>
> - Estos estilos personalizados no deben hallarse en la parte "managed section". De lo contrario, se sobrescriben o confunden a la consola de administración de StoreFront.
> - Los dos estilos especifican el mismo tamaño de fondo. Esto se debe a que el tamaño se especifica en unidades "lógicas", y para la imagen x2, el tamaño de fondo es la mitad del ancho y de la altura del logotipo real.

Establecer una imagen de fondo

> Nota:
>
> La experiencia unificada está diseñada para fondos blancos sencillos. Las imágenes de fondo suelen distraer. Si agrega una imagen de fondo, intente usar una imagen simple. Si fuera necesario, ajuste las fuentes para que sigan funcionando encima de esta imagen.

Ejemplo 1: Referencia CSS a la imagen cargada

Modifique custom.css de la siguiente manera:

```
.storeViewSection {

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

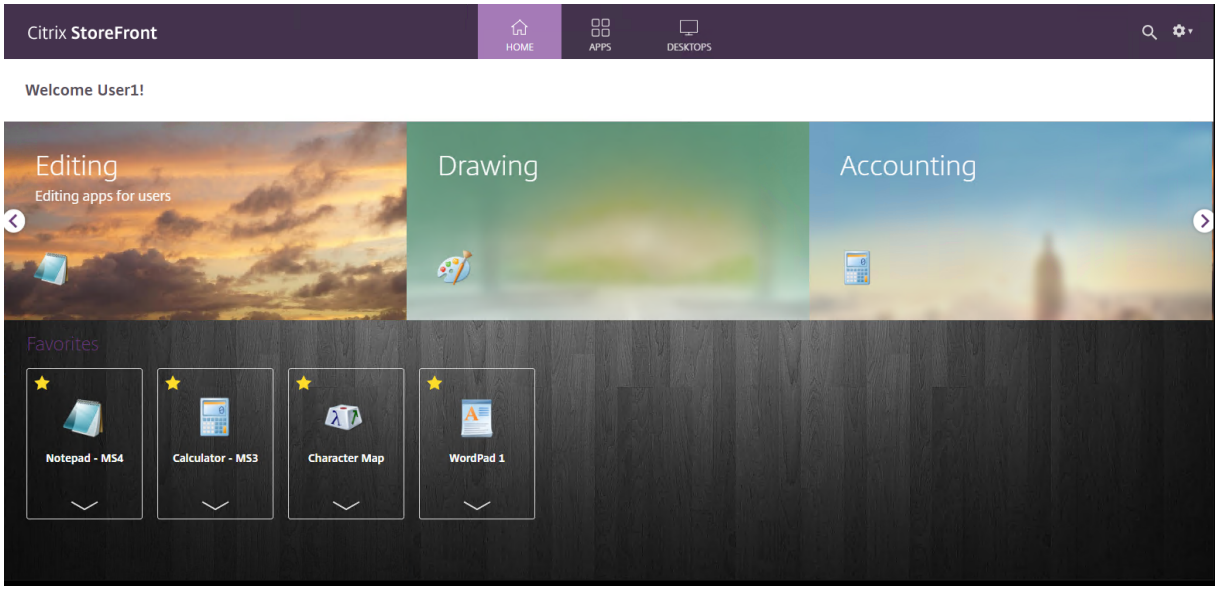

> Nota:
>
> La instrucción background-size:cover; no funciona en algunos exploradores antiguos.

Ejemplo 2: Referencia CSS a la imagen existente con retoques

Modifique custom.css de la siguiente manera:

```
.storeViewSection {

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


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

    color: white;
 }


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

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


.smallTiles .applicationBundleContainer {

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

Esto da el siguiente resultado:



Buscar errores en el código

Hay varias formas de depurar el código. Pruebe siempre con un explorador primero. Esto es mucho más fácil que depurar personalizaciones en la aplicación Citrix Workspace. Puede agregar los siguientes argumentos después de ? o # en la URL de la página, y puede encadenar varios. Por ejemplo:

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

-errors: Normalmente, tratamos de suprimir cualquier error que pueda darse en el código, pero también puede resaltarlos en su lugar. Este argumento muestra un cuadro de alerta cuando se produce un error.

-debug: Este argumento inhabilita cualquier control de excepciones para el código de personalización. Esto es útil con las herramientas de desarrollo integradas en los exploradores modernos (como F12 en Google Chrome o Internet Explorer), y usted depura las excepciones directamente.

-nocustom: Este argumento inhabilita sus personalizaciones de script y CSS. Esto resulta útil si la aplicación Citrix Workspace no funciona y quiere averiguar si se debe a un error que ha introducido usted.

-tr: Este argumento proporciona el seguimiento del código de la interfaz de usuario de la aplicación Citrix Workspace en una ficha separada del explorador, incluido cualquier seguimiento que agregue con llamadas a **CTXS.ExtensionAPI.trace()**.

Experiencia de usuario unificada

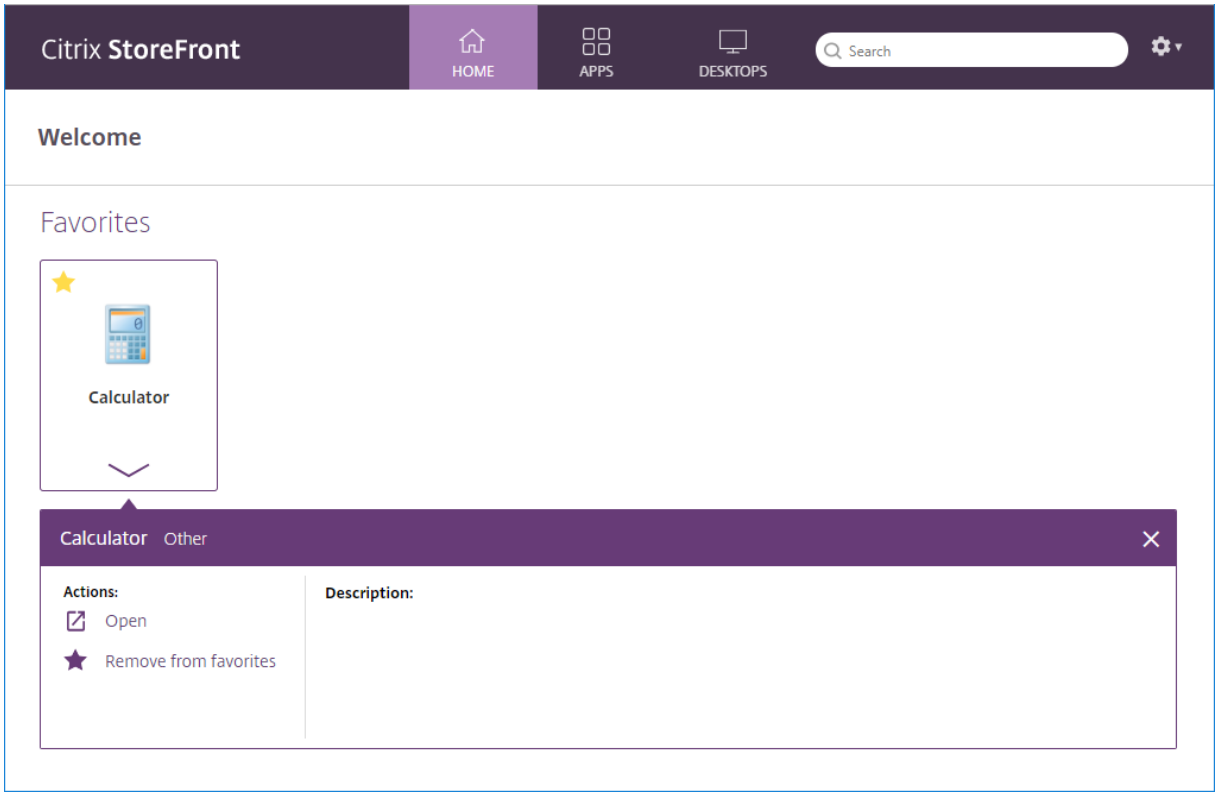
En esta sección se describen las funciones y el aspecto de la experiencia unificada.

Diseño de tarjeta

En el almacén, las aplicaciones se representan en un diseño de “tarjeta”. Puede expandir un panel debajo de cada tarjeta para ver acciones y más detalles.

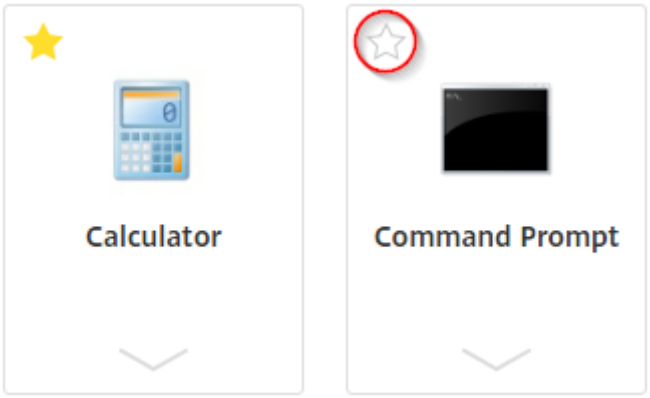
Inicio

Inicio muestra los favoritos.



Favoritos

Haga clic o toque en la estrella para convertir un elemento en favorito:



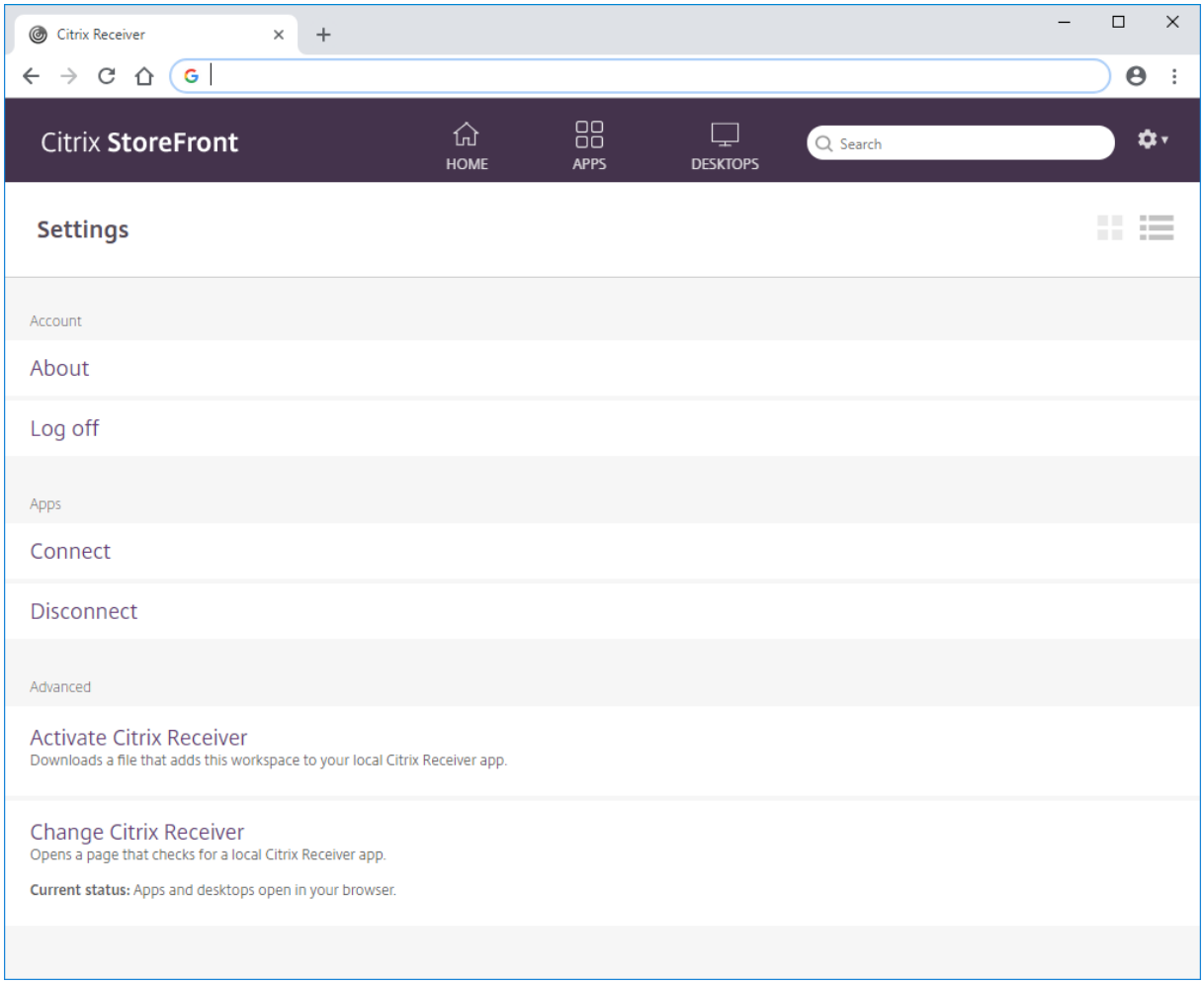
Buscar

Busque en todas las aplicaciones, escritorios y categorías:

Parámetros

Acceda a los parámetros desde el menú desplegable:

En el menú aparece el nombre de usuario, tomado del nombre simplificado de Active Directory. Si el nombre simplificado se ha dejado en blanco (esto no se recomienda), lo que se muestra es el dominio y el nombre de cuenta. Utilice el menú para abrir la página “Parámetros”, consultar la versión de la aplicación Citrix Workspace o cerrar la sesión.



Desde “Parámetros”, puede reanudar las sesiones desconectadas, desconectar todas las sesiones actuales y cerrar la sesión respectivamente. Mostrar la página “Parámetros” como tarjeta o lista:

Conectar. Reanuda las sesiones desconectadas.

Desconectar. Desconecta todas las sesiones actuales y cierra la sesión.

Activar Citrix Receiver. Descarga un archivo que agrega este almacén a la aplicación Citrix Workspace local.

Cambiar Citrix Receiver. Abre una página que busca una aplicación Citrix Workspace local. También permite a los usuarios cambiar entre iniciar recursos mediante la aplicación Citrix Workspace instalada localmente o iniciarlos en un explorador HTML5.

Crear y administrar aplicaciones destacadas

March 2, 2020

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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado,
> propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

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 Almacenes 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 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 para ellos, así como el método mediante el que se definen los grupos de aplicaciones destacadas. Puede elegir entre palabras clave, nombres de las aplicaciones, o categoría de la aplicación. Después, haga clic en **Aceptar**.

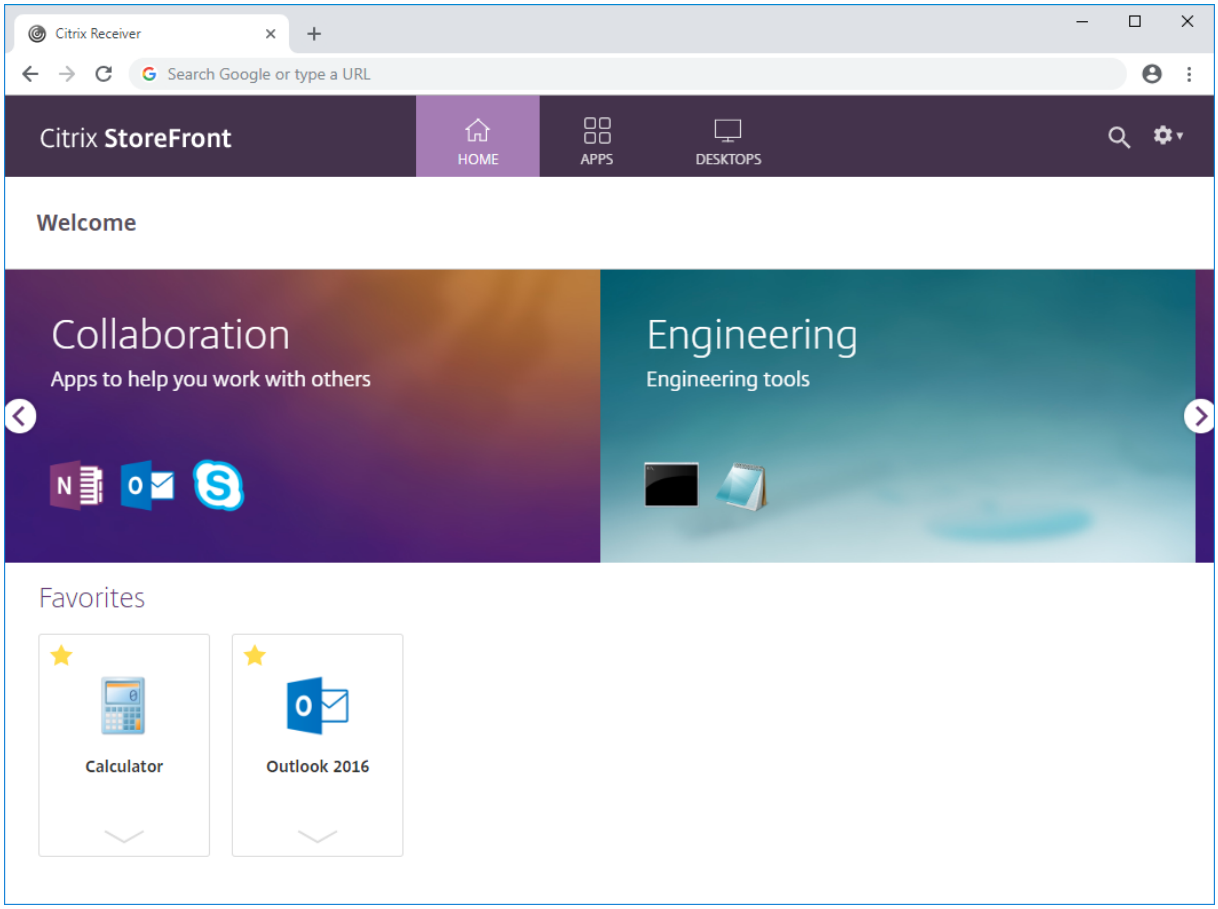
Opción	Descripción
Palabras clave	Defina las palabras clave en Studio.
Categoría de aplicación	Defina la categoría de una aplicación en Studio.

Opción	Descripción
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: Compuesto por aplicaciones de la categoría **Collaboration** de Studio.
- Engineering: Creado al nombrar el grupo de aplicaciones y especificar una colección de nombres de aplicaciones.



Configurar el control del espacio de trabajo

August 22, 2019

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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado, propague los cambios de configuración al grupo de servidores para que se

> actualicen los demás servidores de la implementación.

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 **Almacenes** 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:
   - Habilitar el control del espacio de trabajo
   - Configurar las opciones de reconexión de la sesión
   - Especificar la acción de cierre de sesión

Configurar el uso de fichas del explorador web con la aplicación Citrix Workspace para HTML5

August 22, 2019

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

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

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 **Almacenes** y, en el panel Acciones, seleccione **Administrar sitios de Receiver para Web** y haga clic en **Configurar**.
3. Seleccione **Implementar la aplicación Workspace/Citrix Receiver**.
4. En la lista **Opción de implementación**, seleccione **Usar siempre Receiver para HTML5** y, según la ficha en la que quiera iniciar las aplicaciones, marque o desmarque la opción **Iniciar las aplicaciones en la misma ficha que Receiver para Web**.

Configurar la duración del tiempo de espera en las comunicaciones y los reintentos

March 2, 2020

De forma predeterminada, el tiempo de espera de las solicitudes de un sitio de Citrix Receiver para Web para el almacén asociado se agota pasados tres minutos. El almacén se considera no disponible después de un intento de comunicación fallido. Utilice la tarea **Parámetros avanzados** para cambiar estos 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado, propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

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 **Almacén** en el panel izquierdo de la consola de administración de Citrix StoreFront, seleccione un almacén 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.

Configurar el tiempo de espera de la sesión

Si el tiempo de espera de la sesión no está configurado correctamente en StoreFront, puede que los usuarios vean este mensaje de tiempo de espera: "La sesión agotó el tiempo de espera por inactividad". Puede restablecer el valor del tiempo de espera de la sesión y aumentar el tiempo establecido en el temporizador de inactividad para adaptarlo al uso de los usuarios.

Complete los siguientes pasos para configurar el tiempo de espera de la sesión en StoreFront:

Aumentar el tiempo de espera de la sesión para StoreFront

1. En StoreFront, vaya a **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Busque la entrada **<sessionState timeout="20"/>** en el archivo `web.config`.
3. Cambie **sessionState timeout** al valor pertinente en minutos.

Aumentar la validez máxima del token del servicio de autenticación

Si aumenta el tiempo de espera de la sesión de Citrix Receiver para Web a sea más de una hora, también debe aumentar consecuentemente la validez máxima del token en el **Servicio de autenticación**.

Aumentar el tiempo de espera de sesión para la aplicación Citrix Workspace

1. Para la aplicación Citrix Workspace instalada en el servidor StoreFront, vaya a la ruta del servicio de autenticación de su almacén. En versiones recientes de StoreFront, esta ruta es **c:\inetpub\wwwroot\Citrix\<Store>Auth** (que podría ser uno de varios servicios de autenticación, dependiendo del número de almacenes que tenga).

   En versiones anteriores de StoreFront, la ruta es **c:\inetpub\wwwroot\Citrix\Authentication** (que podrían compartirla los servicios de autenticación o ser la única del servidor).

2. En el archivo `web.config`, busque la entrada **<defaultLifetime="01:00:00"maxLifetime="01:00:00">**.

3. Cambie **maxLifetime** al valor pertinente.

> Nota:
>
> Aplicación Citrix Workspace para Windows y aplicación Citrix Workspace para Linux. Después de cerrar la sesión actual, puede ver Citrix Virtual Apps and Desktops en segundo plano. Sin embargo, después de agotarse el tiempo de espera de la sesión de StoreFront, deberá volver a introducir las credenciales cuando haga clic en cualquier aplicación o escritorio.

Aumentar la validez del token de autenticación

Si quiere un tiempo de espera superior a ocho horas, modifique el archivo `web.config` ubicado en Citrix Receiver para Web para aumentar la validez del token de autenticación:

1. En StoreFront, vaya a **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Localice la entrada **<authentication tokenLifeTime="08:00:00"method="Auto"/>**
3. Cambie **tokenLifeTime** al valor pertinente.

Reiniciar IIS

- Ejecute el comando **iisreset** para aplicar los cambios. La ejecución de este comando cierra la sesión de los usuarios de Citrix Receiver para Web y no afecta a su sesión ICA actual.

> **Nota:**
>
> El formato completo de la validez es `.d.hh:mm:ss[.ff]`. La validez máxima no está limitada a

> 24 horas.

Recursos adicionales

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

Configurar el acceso de los usuarios

March 2, 2020

Configurar que se admitan conexiones a través de las direcciones URL de XenApp Services

Utilice la tarea **Configurar soporte de XenApp Services** para definir el acceso a los almacenes a través de las direcciones URL de XenApp Services. Los usuarios de dispositivos de escritorio reasignados que cuentan con Citrix Desktop Lock, junto con los usuarios que tienen clientes Citrix anteriores que no se pueden actualizar, pueden acceder a los almacenes directamente mediante la URL de XenApp Services de cada almacén. Al crear un almacén, la URL de XenApp Services 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado, propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar soporte de XenApp Services**.
3. Marque o desmarque **Habilitar soporte de XenApp Services** para habilitar o inhabilitar el acceso de los usuarios al almacén mediante la URL de XenApp Services que se muestra.

   La URL de XenApp Services de un almacén tiene el formato `http[s]://<serveraddress>/Citrix/<storename>/PNAgent/config.xml*`, donde *serveraddress* es el nombre de do-

minio completo del servidor o del entorno con carga equilibrada de la implementación de StoreFront, mientras que *storename* es el nombre especificado para el almacén cuando se creó.

4. Si habilita el soporte de XenApp Services, tiene la opción de especificar un almacén predeterminado en la implementación de StoreFront para los usuarios que cuentan con el plug-in de Citrix Online.

   Especifique un **almacén predeterminado**, de modo que los usuarios puedan configurar el plug-in de Citrix Online con la URL del servidor o la URL de equilibrio de carga de la implementación de StoreFront, en lugar de la URL de XenApp Services de un almacén concreto.

Habilitar o inhabilitar la reconexión al control del espacio de trabajo

El control del espacio de trabajo permite que las aplicaciones sigan a los usuarios cuando estos cambian de dispositivo. Esto permite, por ejemplo, que el personal médico en los hospitales pueda 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 al control del espacio de trabajo en el servicio de almacén para la aplicación Citrix Workspace. Puede administrar esta función desde la consola de StoreFront o PowerShell.

Mediante 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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
3. Seleccione **Parámetros avanzados** y marque o desmarque **Permitir la reconexión de sesiones**.

Mediante PowerShell

Cierre la consola de administración y ejecute el siguiente fragmento de código para importar los módulos de PowerShell para StoreFront:

```
$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 al control del espacio de trabajo.

Sintaxis

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

Por ejemplo, para desactivar la reconexión al control del espacio de trabajo en un almacén en */Citrix/Store*, el siguiente comando configura el almacén:

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

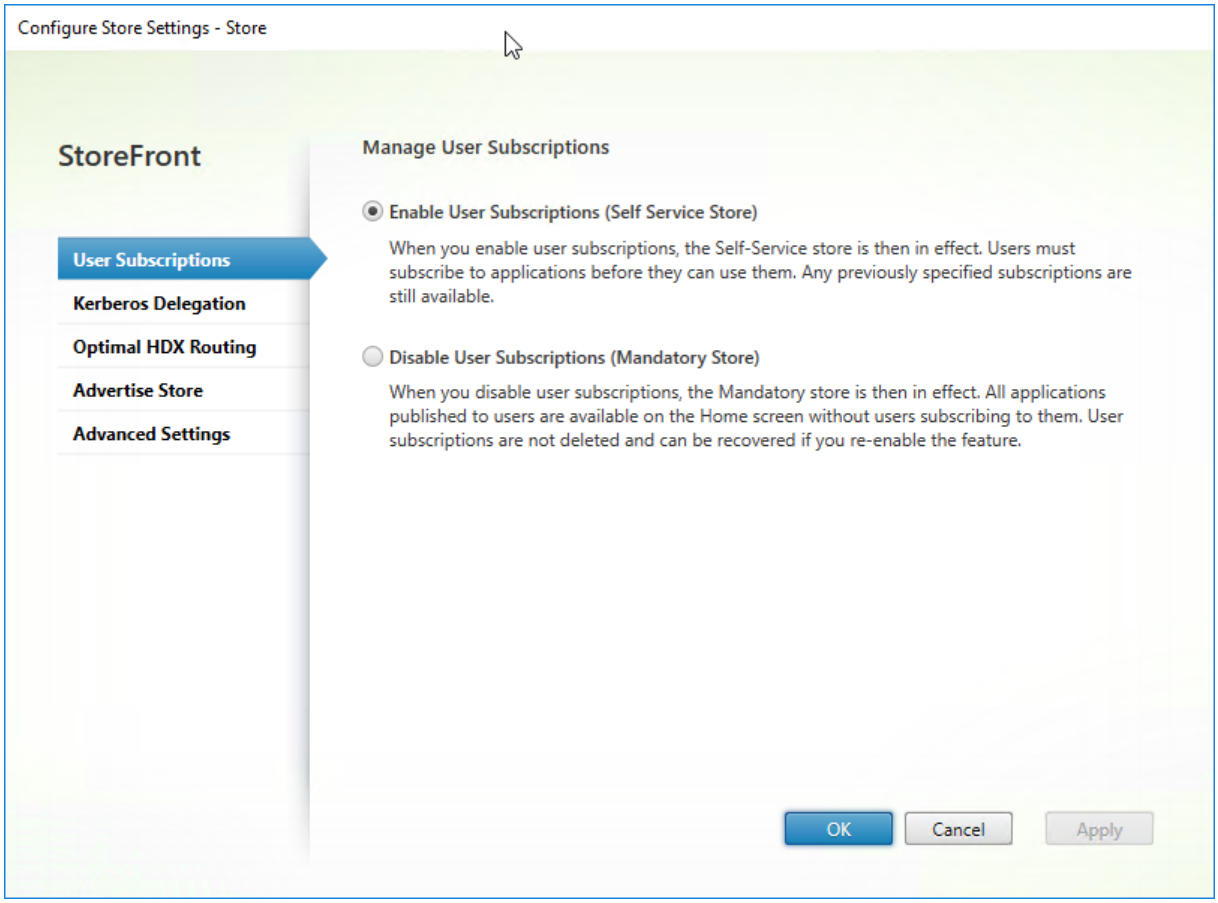
Configurar las suscripciones de los usuarios

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 (almacén de autoservicio).
- Permitir que los usuarios puedan recibir todas las aplicaciones cuando se conectan al almacén (almacén obligatorio).

Inhabilitar las suscripciones de los usuarios a un almacén desde StoreFront también impide que se muestre la ficha Favoritos a los usuarios de la aplicación Citrix Workspace. Inhabilitar las suscripciones no elimina los datos de suscripción al almacén Volver a habilitar las suscripciones al almacén permitirá que un usuario vea las aplicaciones a las que se haya 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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros del almacén** > **Suscripciones de usuarios** para habilitar o inhabilitar la suscripción de usuarios.
3. Elija **Habilitar suscripciones de usuarios (almacén 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 (almacén obligatorio)** 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 función de suscripción.



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

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

Para obtener más información sobre Get-STFStoreService, consulte https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Get-STFStoreService/

Configurar StoreFront para iniciar aplicaciones y escritorios en el modo de ventana

January 6, 2020

Para poder iniciar aplicaciones de manera integrada, StoreFront debe estar disponible en la implementación. Si inhabilita la opción integrada para aplicaciones y escritorios, puede plantearse la posi-

bilidad de iniciar los recursos en el modo de ventana.

A continuación, dispone de un ejemplo de un Bloc de notas publicado. Use el nombre de la aplicación publicada exactamente como se muestra en el conjunto de aplicaciones de la consola de Citrix Virtual Apps and Desktops.

> **Nota:**
>
> En los archivos ICA, la mayoría de los parámetros no distinguen entre mayúsculas y minúsculas, excepto `DesiredHRES` y `DesiredVRES`. Cuando aplique la versión de la aplicación en el modo de ventana, use el nombre del explorador web para hacer referencia a la aplicación en el archivo *default.ica* presente en el servidor de StoreFront. El nombre del explorador perteneciente a la aplicación está disponible en Delivery Controller (debe utilizar PowerShell para verlo):
>
> ```
> >>asnp citrix*
> ```
>
> ```
> >>Get-BrokerApplication -ApplicationName
> ```

Para configurar StoreFront

1. Modifique el archivo default.ica en el servidor de StoreFront que hay en el directorio `\inetpub\wwwroot\Citrix\StoreName\App_Data`.
2. En el archivo default.ica, busque las líneas `[ApplicationServers] application=`.
3. Cree una línea después de `application=` y agregue los siguientes parámetros:

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

4. Guarde el archivo.

Para escritorios publicados desde Citrix Virtual Apps and Desktops 7.x y StoreFront 3.x

1. Modifique el archivo *web.config* en el servidor de StoreFront que hay en el directorio `C:\inetpub\wwwroot\Citrix\storeWeb`.
2. En el archivo web.config, busque la siguiente línea: `showDesktopViewer=''true''`.
3. Modifique el valor de **True** a **False**.
4. En el lado del cliente o desde AD-GPMC, utilice el archivo de plantilla administrativa (`receiver.adm` o `receiver.admx\receiver.adml`, en función del sistema operativo) para configurar la siguiente directiva:
   - **Configuración del equipo > Componentes de Citrix > Citrix Receiver > Experiencia del usuario > Configuración de la presentación del cliente: Habilitar**
   - **Ventanas integradas: False**

- **Anchura de la ventana: <As per requirement>, Altura de la ventana: <As per requirement>**

Notas

DeisredHRES y DesiredVRES se pueden establecer en cualquier resolución; por ejemplo, 800 x 600 o 1024 x 768.

Si la aplicación debe ejecutarse en un porcentaje del tamaño de la pantalla, después de configurar TWIMode=Off, agregue la línea ScreenPercent=90, que configura la pantalla al 90 por ciento. También puede lograr esto con el sitio de XenApp Services. Compruebe que se haya modificado el archivo correspondiente, ubicado en la carpeta conf de ese sitio (Inetpub\wwwroot\Citrix\PNAgent\conf).

Si está utilizando el cliente 10.x y modifica el archivo **default**.ica o template.ica, agregue solo la línea TWIMode=Off. Con ella, obtiene los parámetros HRES y VRES desde las propiedades de la aplicación publicada. De lo contrario, aparece un error que indica entradas duplicadas en el archivo ICA cuando un usuario intenta iniciar la aplicación.

Configurar almacenes multisitio con alta disponibilidad

January 6, 2020

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

Para los almacenes 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 Citrix Gateway para sus implementaciones, puede definir el dispositivo óptimo para el acceso de los usuarios a cada una de las implementaciones.

Configurar la combinación y la 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.
- **Implementaciones agrupadas:** Puede especificar qué implementaciones tienen los recursos que quiera agregar. Los recursos coincidentes procedentes de implementaciones agrupadas se presentan al usuario como un único recurso con alta disponibilidad.
- **Asociar una zona a una implementación:** Cuando se accede con Citrix Gateway en una configuración de equilibrio de carga global, StoreFront prioriza las implementaciones de las zonas que coinciden con la zona de la puerta de enlace cuando se inician los recursos.

1. Compruebe que ha configurado el almacén con información de todas las implementaciones de Citrix Virtual Apps and Desktops que quiera usar en la configuración. Para obtener más información sobre cómo agregar implementaciones a almacenes, consulte Administrar los recursos disponibles en los almacenes.
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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y haga clic en **Administrar Delivery Controllers** en el panel **Acciones**.
4. Si se definen dos o más controladores, haga clic en **Asignación de usuarios y Configuración de la agrupación multisitio> Configurar**.
5. Haga clic en **Asignar usuarios a controladores** 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** para agrupar recursos de varias implementaciones. Cuando se agrupan Delivery Controllers, las aplicaciones y los escritorios de dichos Delivery Controllers que tengan el mismo nombre simplificado y la misma ruta se presentarán como una sola aplicación o escritorio en la aplicación Citrix Workspace.
   a) Para agrupar Delivery Controllers, seleccione varios Controllers y haga clic en **Agrupar**.
   b) Seleccione estas opciones de **Parámetros de Controllers agrupados**:

      Los Controllers publican recursos idénticos: Al seleccionar esta opción, StoreFront enumera los recursos de solo uno de los Controllers agrupados. Si no se selecciona, StoreFront enumera los recursos de todos los Controllers agrupados (para acumular todo el conjunto de recursos disponibles del usuario). Seleccionar esta opción 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: Al seleccionar esta opción, los inicios de recursos se distribuyen de forma uniforme entre los Controllers disponibles. Si no se selecciona, 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.

7. En el cuadro de diálogo Configuración de la agrupación multisitio y la asignación de usuarios, haga clic en **Aceptar**.
8. En el cuadro de diálogo Administrar Delivery Controllers, haga clic en **Aceptar**.

Configuraciones avanzadas

Puede configurar muchas operaciones comunes multisitio y de alta disponibilidad con la consola de administración de StoreFront. También puede configurar StoreFront mediante PowerShell o si modifica los archivos de configuración de StoreFront, lo que ofrece las siguientes funcionalidades adicionales:

- 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 almacenes con implementaciones que tengan conjuntos de recursos dispares, se pueden conseguir mejoras al aplicar 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.

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

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



```
</resourcesWingConfigurations>
```

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

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

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 *domain\usergroup* (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 y equilibrar la carga o conmutar 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 cualquier momento. Especifique los nombres de los grupos de combinación 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 combinación 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 combinación con la 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 del atributo **identical** es **false**, aunque cambia a **true** cuando StoreFront se actualiza, para evitar que se modifique el comportamiento después de una actualización.
- **primaryFarmRefs:** Especifica un conjunto de sitios equivalentes de Citrix Virtual Apps and

Desktops donde coinciden todos o algunos de los recursos. Escriba los nombres de las implementaciones que ya se han agregado al almacén. Los nombres de las implementaciones que especifique deben coincidir exactamente con los nombres que ha especificado al agregar las implementaciones al almacén.

- **optimalGatewayForFarms:** Especifica grupos de implementaciones y define los dispositivos Citrix 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 Citrix Gateway óptimos para implementaciones donde el dispositivo a través del cual los usuarios acceden a StoreFront no es el mejor.

Configurar la sincronización de suscripciones

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

> **Nota:**
>
> 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.

Cuando establezca la sincronización de las suscripciones, tenga en cuenta que los Delivery Controllers configurados deben nombrarse de manera idéntica en todos los almacenes sincronizados y que los nombres del Delivery Controller distinguen entre mayúsculas y minúsculas. Si no duplica el nombre exacto de los Delivery Controllers se pueden crear suscripciones diferentes para los usuarios en los almacenes sincronizados. Si sincroniza suscripciones a partir de recursos agregados, el nombre de los grupos de agregación utilizados por ambos almacenes también debe coincidir. Los nombres de Delivery Controller y de grupos de agregación distinguen entre mayúsculas y minúsculas; por ejemplo, *XenDesktop7* es distinto de *Xendesktop7*.

1. Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell ISE.
2. Si quiere configurar la sincronización para que se produzca en un momento determinado todos los días, ejecute el siguiente comando

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

   Utilice **-StartTime** para especificar cuándo se debe iniciar la programación de sincronización.

Con **(Get-Date -Format t)**, la programación de sincronización se inicia inmediatamente, mientras que al especificar *10:00* la programación se inicia a la hora especificada.

-RepeatMinutes establece la frecuencia con la que se ejecutará la programación. Por ejemplo, *30* ejecuta la programación cada media hora y *180* ejecuta la programación cada 3 horas. Se recomienda escalonar las programaciones de extracción para evitar que dos grupos de servidores intenten extraer datos de suscripción entre sí al mismo tiempo. Por ejemplo, una programación para extraer datos de cada grupo de servidores cada 60 minutos se configuraría de la siguiente manera. El grupo de servidores 1 extrae datos del grupo de servidores 2 a las horas 01:00, 02:00, 03:00, etc. El grupo de servidores 2 extrae datos del grupo de servidores 1 a las horas 01:30, 02:30, 03:30, etc.

3. Para especificar la implementación remota de StoreFront que contiene el almacén que se sincronizará, escriba el siguiente comando Debe configurar esto para cada centro de datos en el que reside un grupo de servidores de StoreFront, de manera que pueda extraer datos de suscripción de otros centros de datos remotos. Consulte los siguientes ejemplos de centros de datos de EE. UU. y Reino Unido:

   - Proceso en servidores de StoreFront del centro de datos de Estados Unidos para extraer datos de los servidores del centro de datos del Reino Unido:

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

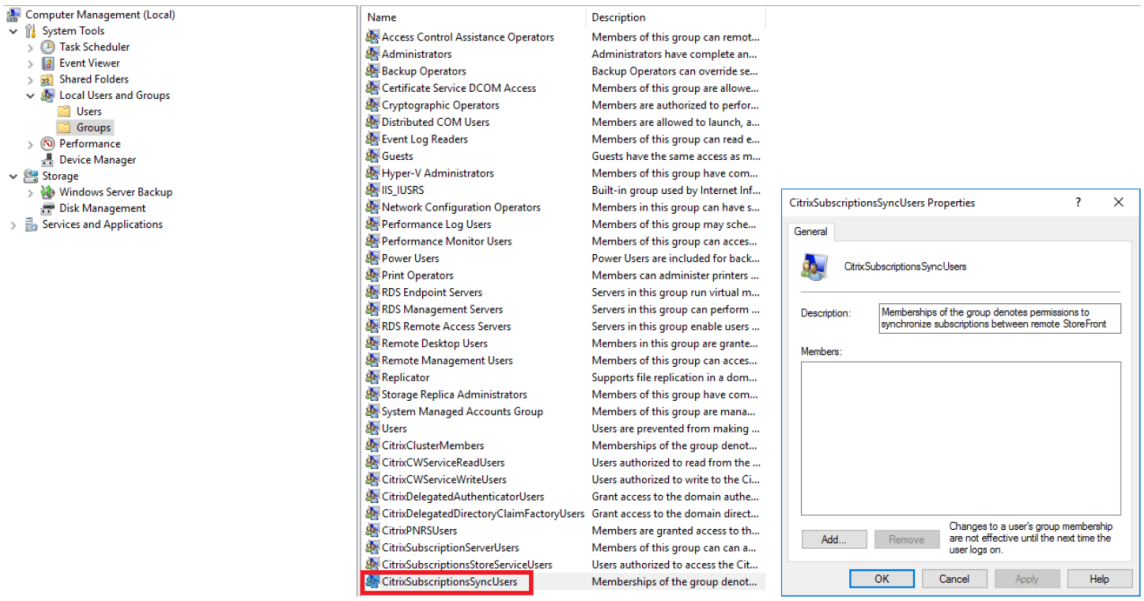
   - Proceso en servidores de StoreFront del centro de datos del Reino Unido para extraer datos de los servidores del centro de datos de Estados Unidos:

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

   donde *FriendlyName* es un nombre que le ayuda a identificar la implementación remota y *RemoteStoreFrontAddress* es el nombre de dominio completo (FQDN) del servidor de StoreFront o grupo de servidores con equilibrio de carga para la implementación remota. Para sincronizar suscripciones a aplicaciones entre dos o más almacenes, todos los almacenes que se van a sincronizar deben tener el mismo nombre en sus respectivas implementaciones de StoreFront.

4. Agregue las cuentas de máquina del dominio de Microsoft Active Directory para cada servidor de StoreFront en la implementación remota al grupo de usuarios local de Windows CitrixSubscriptionSyncUsers en el servidor actual.

   Esto permite a los servidores actuales extraer datos de suscripción nuevos o actualizados de los servidores remotos enumerados en CitrixSubscriptionSyncusers una vez que se haya configurado una programación de sincronización. Para obtener más información sobre la modificación de grupos de usuarios locales, consulte http://technet.microsoft.com/en-us/library/cc772524.aspx.



5. Cuando haya configurado la programación como desee, utilice la consola de administración de Citrix StoreFront, o PowerShell más adelante, para propagar las programaciones y orígenes de sincronización de suscripciones a todos los demás servidores del grupo.

```
1 Publish-STFServerGroupConfiguration
```

   Para obtener más información acerca de la propagación de cambios en una implementación con varios servidores de StoreFront, consulte Configurar grupos de servidores.

6. Para quitar una programación de sincronización de suscripciones, ejecute el siguiente comando y, a continuación, propague el cambio de configuración por el resto de los servidores de StoreFront de la implementación.

```
1 Clear-STFSubscriptionSynchronizationSchedule
```

7. Para quitar un origen de sincronización de suscripciones específico, ejecute el siguiente comando y, a continuación, propague el cambio de configuración a los demás servidores de StoreFront de la implementación.


```
Remove-STFSubscriptionSynchronizationSource -FriendlyName "
    SyncFromUKStore"
```

8. Para quitar todos los orígenes de sincronización de suscripciones existentes, ejecute el siguiente comando y, a continuación, propague el cambio de configuración a los demás servidores de StoreFront de la implementación.

```
Clear-STFSubscriptionSynchronizationSource
```

9. Para enumerar las programaciones de sincronización de suscripciones configuradas actualmente para su implementación de StoreFront, ejecute el siguiente comando.

```
Get-STFSubscriptionSynchronizationSchedule
```

10. Para enumerar los orígenes de sincronización de suscripciones configuradas actualmente para su implementación de StoreFront, ejecute el siguiente comando.

```
Get-STFSubscriptionSynchronizationSource
```

Configurar el enrutamiento HDX óptimo para un almacén

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

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 Citrix Virtual Apps and Desktops en varias zonas basándose en el centro de datos o la ubicación geográfica donde residen los Controllers de Citrix Virtual Apps and Desktops y los recursos publicados. Defina las zonas en Citrix Virtual Apps and Desktops Studio. StoreFront funciona en combinación con Citrix Virtual Apps and Desktops, y las zonas que se definan en StoreFront deben coincidir exactamente con los nombres de zona definidos en Citrix Virtual Apps and Desktops.

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 mediante comunidades de servidores, la cual podría resultarle familiar. 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 Citrix Virtual Apps and Desktops. 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

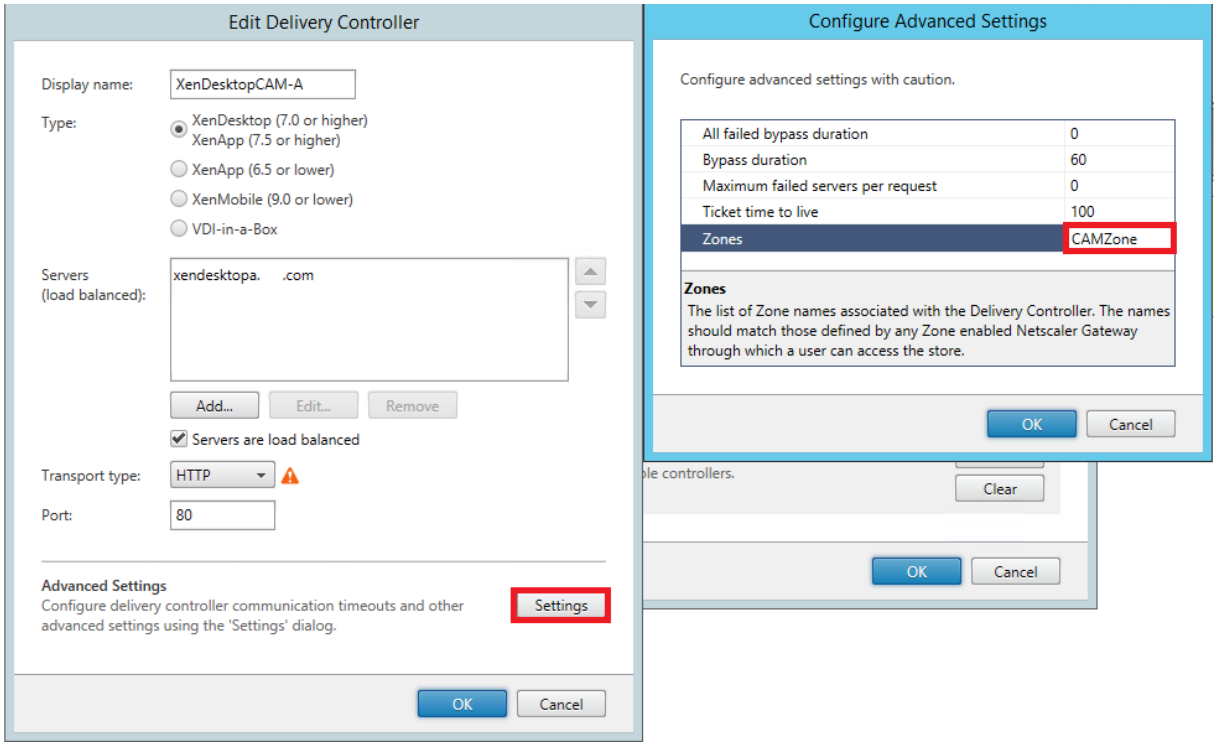
centro de datos en una ubicación geográfica. Es de esperar que cada zona tenga como mínimo un dispositivo Citrix Gateway óptimo que se utiliza para conexiones HDX con los recursos de esa zona.

Para obtener más información sobre las zonas, consulte Zonas.

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y haga clic en **Administrar Delivery Controllers** en el panel **Acciones**.
3. Seleccione un Controller, haga clic en **Modificar** y luego en **Parámetros** en la pantalla **Modificar Delivery Controller**.
4. En la fila de **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 Citrix Gateway para mejorar el control del enrutamiento de la conexión ICA desde el motor HDX a los recursos publicados, tales como los VDA de XenDesktop o las aplicaciones publicadas de Citrix Virtual Apps and Desktops mediante StoreFront. Por regla general, la puerta de enlace óptima para un sitio se coloca en la misma ubicación geográfica.

Solo necesita definir los dispositivos Citrix 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 EE. UU., solo en caso de que fallen los del Reino Unido

1 x Puerta de enlace en EE. UU. –> 1 x StoreFront en EE. UU.

- Aplicaciones y escritorios locales en EE. UU.
- Aplicaciones y escritorios locales en Reino Unido, solo en caso de fallo de los de EE. UU.

Una puerta de enlace del Reino Unido proporciona acceso remoto a recursos alojados en el Reino Unido, como aplicaciones y escritorios que utilicen un StoreFront del Reino Unido.

El almacén de StoreFront del Reino Unido tiene definidas, en su lista de Delivery Controllers, puertas de enlace Citrix Gateway basadas tanto en Reino Unido como en Estados Unidos y Controllers también en ambos países. 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 conectarse a recursos de EE. UU. como solución temporal.

Sin un enrutamiento de puerta de enlace óptima, todos los inicios ICA pasarían a través de la puerta de enlace del Reino Unido que realizó la solicitud de inicio, independientemente de la ubicación geográfica de 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 EE. UU. a través de la puerta de enlace más próxima a las comunidades de EE. UU. que ofrecen los escritorios y aplicaciones.

> **Nota:**
>
> Solo se puede asignar una puerta de enlace óptima por sitio, para cada almacén de StoreFront.

Ejemplo de uso con zonas

1 x ZonaCAM -> 2 x StoreFronts en Reino Unido

- Cambridge, Reino Unido: Aplicaciones y escritorios
- Fort Lauderdale, Costa Este de EE. UU.: Aplicaciones y escritorios
- Bangalore, India: Aplicaciones y escritorios

1 x ZonaFTL -> 2 x StoreFronts en EE. UU.

- Fort Lauderdale, Costa Este de EE. UU.: 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, Costa Este de EE. UU.: Aplicaciones y escritorios

Figura 1. Enrutamiento no óptimo de la puerta de enlace

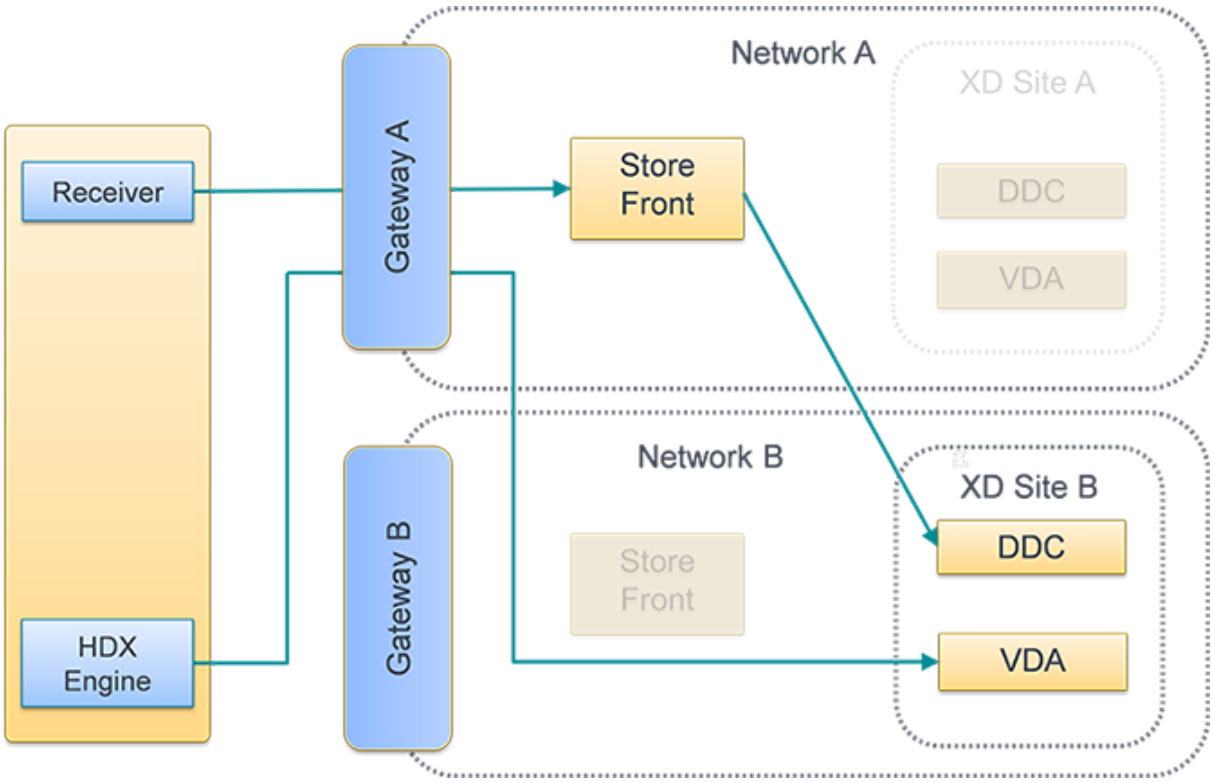
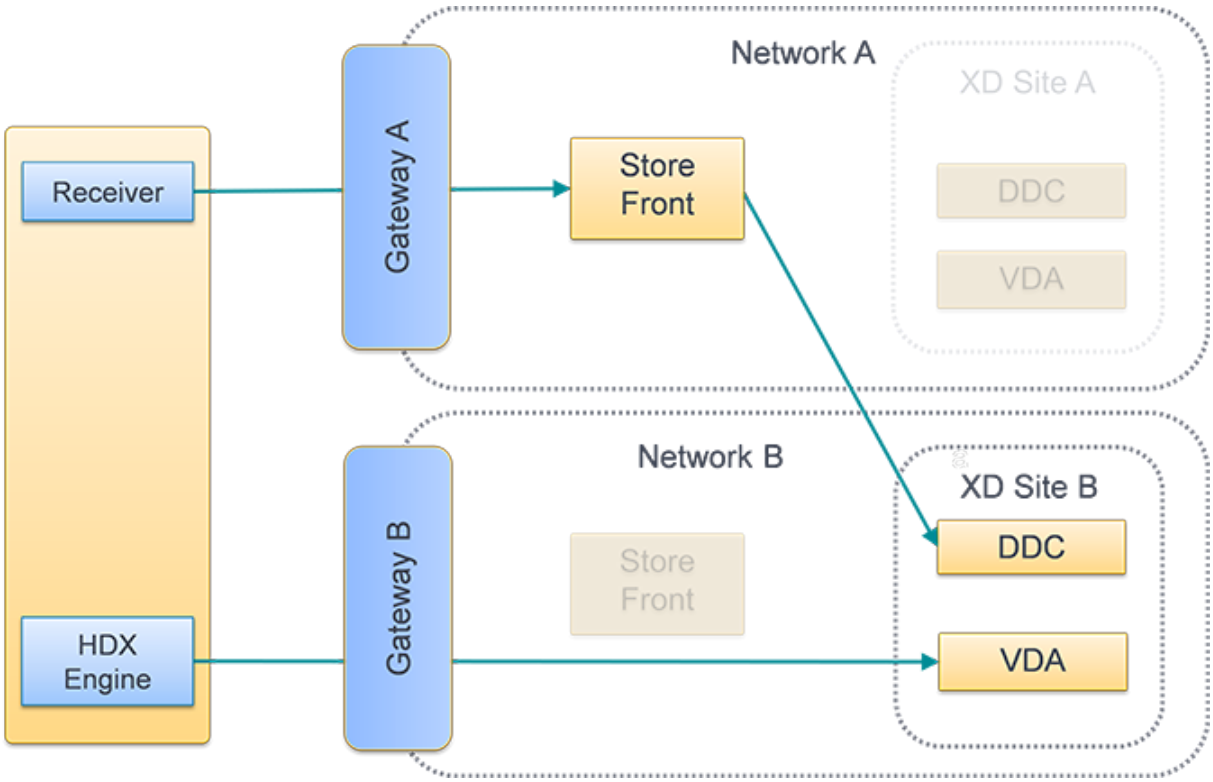


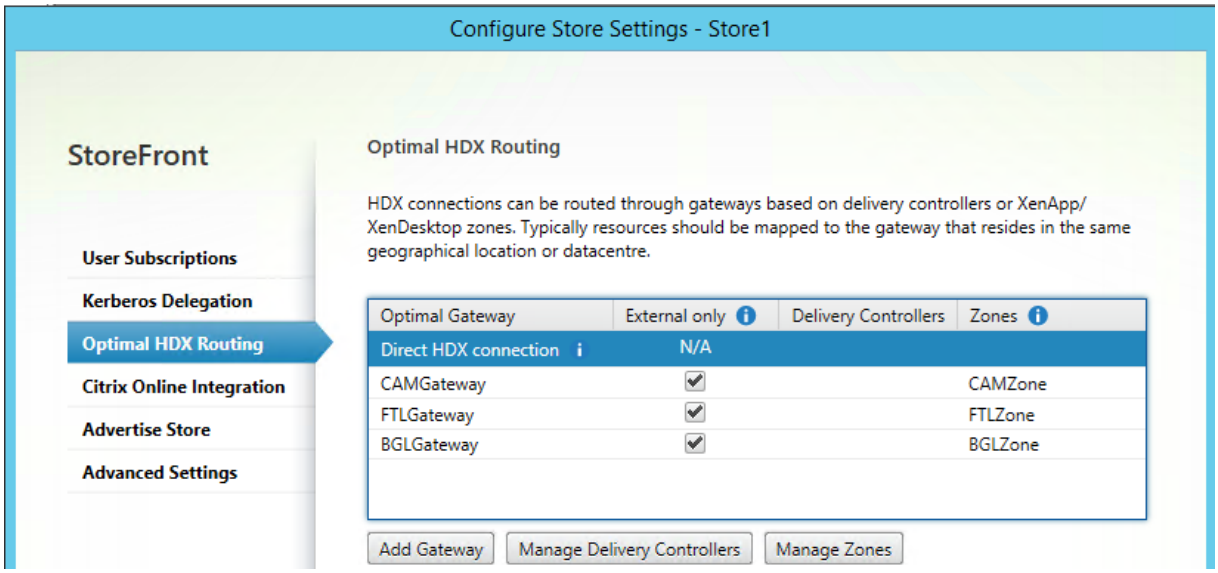
Figura 2. Enrutamiento óptimo de la puerta de enlace



Usar la consola de administración de Citrix StoreFront

Después de haber configurado diferentes dispositivos Citrix 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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
3. En la página **Parámetros** > **Enrutamiento óptimo de HDX**, seleccione una puerta de enlace.
4. Si selecciona la casilla de verificación **Solo externo**, es equivalente a **-enabledOnDirectAccess = false** y la Conexión HDX directa es equivalente a usar **Set-DSFarmsWithNullOptimalGateway** para zonas o comunidades.



Agregar una 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 Citrix Gateway.

1. En la pantalla **Parámetros generales**, complete los parámetros Nombre simplificado, URL de Citrix Gateway y Uso o rol para configurar el acceso a los almacenes a través de Citrix Gateway para los usuarios que se conectan desde redes públicas. El acceso remoto mediante Citrix Gateway no se puede aplicar a almacenes no autenticados.
2. En la pantalla **Secure Ticket Authority (STA)**, complete las opciones que se muestran. STA está alojado en servidores Citrix Virtual Apps and Desktops. Emite tíquets de sesión en respuesta a las solicitudes de conexión. Esos tíquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de Citrix Virtual Apps and Desktops.
3. En la pantalla **Parámetros de autenticación**, introduzca los parámetros que especifican cómo el usuario remoto proporciona las credenciales de autenticación.

Usar PowerShell para configurar el enrutamiento óptimo de Citrix Gateway para un almacén

Parámetros de API de PowerShell

-SiteId (entero): ID del sitio dentro de IIS. Normalmente es 1 para el sitio en IIS donde StoreFront se instala de manera predeterminada.

-ResourcesVirtualPath (cadena): Ruta del almacén que se va a configurar para tener una comunidad para la asignación de puerta de enlace óptima.

Ejemplo: “/Citrix/Store”

-GatewayName (cadena): Nombre proporcionado para identificar al dispositivo Citrix 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 Citrix Gateway óptimo.

Ejemplo 1 para el puerto estándar 443 de un servidor virtual: `gateway.example.com`

Ejemplo 2 para el puerto no estándar 500 de un servidor virtual: `gateway.example.com:500`

-Farms (matriz de cadenas): Especifica un conjunto de implementaciones, normalmente colocadas en una misma ubicación, de Citrix Virtual Apps and Desktops que comparten el mismo dispositivo Citrix Gateway óptimo. Las comunidades pueden contener uno o más Delivery Controllers que ofrecen recursos publicados.

Puede configurar un sitio de Citrix Virtual Desktops 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-B.example.com`

`XenDesktop-C.example.com`

-Zones (matriz de cadenas): Especifica un centro de datos o varios centros de datos que contienen varios 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 Citrix Virtual Apps and Desktops que ejecutan Secure Ticket Authority (STA). Si usa varias comunidades, incluya los servidores STA en cada una de ellas mediante 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 tíquets de sesión de todos los STA, y distribuye 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 que aparecen en la configuración, lo que reduce la cantidad 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 reconectarse automáticamente. Si ha configurado varios STA y quiere asegurarse de que la fiabilidad de la sesión está siempre disponible, establezca el valor del atributo useTwoTickets en **true** para obtener tíquets de sesión de dos STA diferentes si un STA no está disponible durante la sesión.

-UseTwoTickets (booleano): Si tiene el valor **true**, obtiene tíquets 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 a sus recursos se siguen redirigiendo a través del dispositivo óptimo definido para la comunidad. Si tiene el valor **false**, las conexiones a los recursos no se redirigen a través del dispositivo óptimo de la comunidad, a menos que los usuarios accedan a StoreFront mediante Citrix Gateway.

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

> **Sugerencia:**
>
> 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.

Configurar 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 Optimal Gateway For Farms para el almacén **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
```

Configurar una puerta de enlace óptima para una zona

Ejemplo

Cree o sobrescriba las asignaciones de puerta de enlace óptima para comunidades en la zona **CAM-Zone**.

```
**& "$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 el almacén llamado **Internal**.

```
Get-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath ”/Citrix/
Internal”
```

Ejemplo

Quite todas las asignaciones de puerta de enlace óptima para comunidades para el almacén llamado **Internal**.

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath ”/Citrix/
Internal”
Configure direct HDX connections for farms
```

Ejemplo

Este script impide que los inicios de ICA pasen a través de una puerta de enlace para la lista de comunidades especificadas para el almacén llamado **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 ICA a través de una puerta de enlace para el almacén llamado **Internal**.

```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath ”/Citrix/
Internal”
```

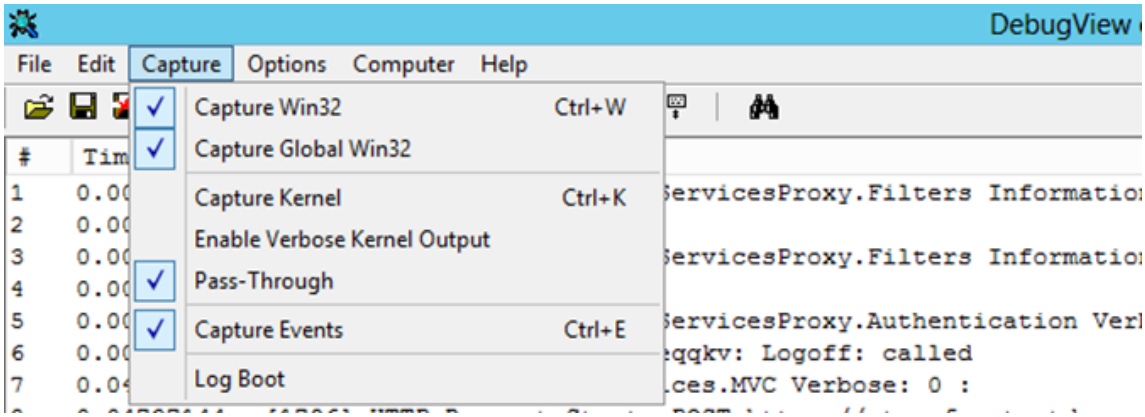

Determinar si StoreFront está usando las asignaciones de puerta de enlace óptima para comunidades

1. Ejecute este comando para habilitar el seguimiento de StoreFront en todos los nodos del grupo de servidores que utilizan PowerShell:

```
& ”$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 de StoreFront. Si está usando un grupo de servidores de 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 de StoreFront.

```
Set-DSTraceLevel -All -TraceLevel Off
```

Casos 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**.
```



```
2
3       'Set-DSOptimalGatewayForFarms -onDirectAccess=false'
4
5       Farm2 está configurada para usar la puerta de enlace óptima
           Gateway2.
6
7       Farm2 tiene inhabilitado el uso de puerta de enlace óptima cuando
           el acceso es directo.
8
9       Se usará la puerta de enlace óptima Gateway2 para el inicio.
10
11  -   Un cliente interno inicia sesión desde StoreFront. El inicio se
       redirige a través de la puerta de enlace óptima designada Gateway1
       para la comunidad Farm1.
12
13      'Set-DSOptimalGatewayForFarms -onDirectAccess=true'
14
15      No se identifica dinámicamente ninguna puerta de enlace durante la
           solicitud. Se ha contactado con StoreFront de manera directa.
16
17      Farm1 está configurada para usar la puerta de enlace óptima
           Gateway1.
18
19      Farm1 tiene habilitado el uso de puerta de enlace óptima cuando el
           acceso es directo.
20
21      Se usará la puerta de enlace óptima Gateway1 para el inicio.
22
23  -   Un cliente interno inicia sesión desde Gateway1. Se impide el paso
       de inicios de recursos en Farm1 a través de cualquier puerta de
       enlace y se contacta con StoreFront directamente.
24
25      'Set-DSFarmsWithNullOptimalGateway'
26
27      Se identifica dinámicamente la puerta de enlace durante la
           solicitud: Gateway1
28
29      Farm1 está configurada para no usar ninguna puerta de enlace. No se
            usará ninguna puerta de enlace para el inicio.
```


Integrar en Citrix Gateway y Citrix ADC

January 6, 2020

Puede utilizar Citrix Gateway con StoreFront para ofrecer acceso remoto seguro a usuarios que se encuentren fuera de la red de la empresa. Asimismo, puede utilizar Citrix ADC para equilibrar la carga.

Planificar el uso de la puerta de enlace y el servidor de certificados

La integración de StoreFront en Citrix Gateway y Citrix ADC 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 `example.com` (externo) y `example.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 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 admitir 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 de 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 de 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 Citrix Virtual Apps and Desktops, que proporcionan recursos equivalentes.
- Planifique el almacenamiento de claves privadas protegidas por hardware. Las puertas de enlace y los servidores, incluidos algunos modelos de Citrix ADC, 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 implementa GSLB con Citrix Gateway, puede que cada puerta de enlace del grupo de equilibrio de carga GSLB deba tener un certificado idéntico, que contiene todos los nombres FQDN que quiera usar.

Para obtener más información sobre cómo proteger su implementación de Citrix, consulte la guía Cifrado de extremo a extremo con Citrix Virtual Apps and Desktops y la sección Protección de Citrix Virtual Apps and Desktops.

Configurar el inicio de sesión en StoreFront cuando la autenticación está inhabilitada en el servidor virtual de Citrix Gateway

Inicie sesión en StoreFront cuando la autenticación esté inhabilitada en la dirección VIP de Citrix Gateway. Este procedimiento funciona en dos casos:
Redes internas. El inicio de aplicaciones falla desde ubicaciones remotas porque los STA no se pueden usar cuando la autenticación se inhabilita en Citrix Gateway si el encabezado X-Citrix-Gateway se está enviando a StoreFront.
Citrix Receiver para Web. Los clientes de Receiver no se autentican si la autenticación no está habilitada en el servidor virtual de Citrix Gateway.

Cambios en el servidor de StoreFront

1. Inhabilite el campo **Requerir coherencia de token**:
   - StoreFront 3.0
     a) Modifique el archivo `web.config` referente al sitio web del almacén. Por ejemplo, si el nombre de un almacén de StoreFront es `NoAuth`, el campo `web.config` en el servidor de StoreFront tendrá la ruta **inetpub\wwwroot\Citrix\NoAuth**.

   a) Busque la siguiente línea en el archivo `web.config` y cambie el valor de “True” a “False”.
   Antes
   `<resourcesGateways requireTokenConsistency=”true”>`

Después

```
<resourcesGateways requireTokenConsistency="false">
```

> **Nota:**
>
> En StoreFront 3.x, el campo **Requerir coherencia de token** es una casilla en la interfaz gráfica de usuario. Para obtener más información, consulte Parámetros avanzados de los almacenes.

b) Guarde el archivo `web.config` y reinicie el servicio IIS.

2. Abra la **consola de administración de Citrix StoreFront**.
3. Haga clic en **Administrar sitios de Receiver para Web** para la web.
4. Seleccione el sitio de Citrix Receiver para Web correspondiente, haga clic en **Configurar** y, a continuación, seleccione **Métodos de autenticación**.
5. Compruebe que la casilla **PassThrough desde Citrix Gateway** no está marcada.

> **Nota:**
>
> Se presupone que Citrix Gateway y "Habilitar acceso remoto" están definidos en el servidor de StoreFront.

Cambios en Citrix Gateway

1. Abra el servidor virtual de Citrix Gateway.
2. Haga clic en la ficha **Authentication** y compruebe que la casilla **Enable Authentication** no está marcada.
3. Vincule la directiva de la sesión correspondiente al servidor virtual de Citrix Gateway.
4. Pruebe la conexión.

Agregar una conexión de Citrix Gateway

January 6, 2020

Utilice la tarea Agregar dispositivo Citrix Gateway para agregar implementaciones de Citrix Gateway a través de las cuales los usuarios podrán acceder a los almacenes. Debe habilitar el método de autenticación PassThrough desde Citrix Gateway antes de poder configurar el acceso remoto a los almacenes a través de Citrix Gateway. Para obtener más información sobre cómo configurar Citrix Gateway para StoreFront, consulte Usar WebFront para la integración con StoreFront.

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

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 **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel Acciones, haga clic en **Administrar Citrix Gateway**.
3. Haga clic en **Agregar** y, en la página Parámetros generales, especifique un **nombre simplificado** para la implementación de Citrix 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 Citrix 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) de la implementación de StoreFront debe ser único y diferente del FQDN del servidor virtual de Citrix Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de Citrix 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 Citrix 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 Citrix 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 Citrix 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 quiere agregar un dispositivo con Citrix Gateway, seleccione en la lista Tipo de inicio de sesión el método de autenticación configurado en el dispositivo para los usuarios de la aplicación Citrix Workspace.

La información que proporcione sobre la configuración de su dispositivo Citrix Gateway se agrega al archivo de aprovisionamiento para el almacén. Eso permite que la aplicación Citrix Workspace 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. Si quiere agregar un clúster, haga clic en Siguiente y continúe en el paso 9.

8. Si quiere configurar StoreFront para Citrix Gateway o un único dispositivo Access Gateway 5.0, complete la URL del servicio de autenticación de Citrix 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 Citrix Gateway para verificar que las solicitudes recibidas desde Citrix 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 los

almacenes.

11. En todas las implementaciones, para que los recursos proporcionados por Citrix Virtual Apps and Desktops estén disponibles en el almacén, enumere en la página Secure Ticket Authority (STA) las direcciones URL de los servidores con 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 Citrix Virtual Apps and Desktops. Emite tíquets de sesión en respuesta a las solicitudes de conexión. Esos tíquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de Citrix Virtual Apps and Desktops.

12. Si quiere que Citrix Virtual Apps and Desktops mantenga abiertas las sesiones desconectadas mientras la aplicación Citrix Workspace intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y quiere asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tíquets de dos STA, si están disponibles.

    Cuando la casilla Solicitar tíquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tíquets 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 Citrix Gateway. Una vez que la implementación se haya agregado, haga clic en **Finalizar**.

    Para obtener más información sobre la actualización de la información de las implementaciones, consulte Configurar parámetros de conexión de Citrix Gateway.

Para proporcionar acceso a los almacenes a través de Citrix Gateway, se necesita una baliza interna y al menos dos balizas externas. La aplicación Citrix Workspace 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 Citrix Gateway que usted agrega se utilizan como balizas externas de forma predeterminada. Para obtener más información sobre el cambio de balizas, consulte Configurar balizas.

Para permitir que los usuarios accedan a los almacenes a través de Citrix Gateway, debe configurar el acceso de usuarios remotos para dichos almacenes.

Importar un dispositivo Citrix Gateway

January 31, 2020

Los parámetros de acceso remoto configurados en la consola de administración de Citrix Gateway deben ser idénticos a aquellos configurados en StoreFront. Este artículo muestra cómo importar los detalles de un servidor virtual de Citrix Gateway para que Citrix Gateway y StoreFront estén configurados correctamente para funcionar juntos.

Requisitos

- Se necesita NetScaler 11.1.51.21, o una versión posterior para exportar varios servidores virtuales de puerta de enlace a un archivo ZIP.

  > **Nota:**
  >
  > Los dispositivos Citrix ADC solo pueden exportar servidores virtuales de puerta de enlace creados mediante el asistente de Citrix Virtual Apps and Desktops.

- DNS debe ser capaz de resolver todas las URL de los servidores STA (Secure Ticket Authority), y StoreFront debe ser capaz de contactar con ellas. Estas direcciones figuran en el archivo GatewayConfig.json en el archivo ZIP generado por el dispositivo Citrix ADC.
- El archivo GatewayConfig.json dentro del archivo ZIP generado por el dispositivo Citrix ADC debe contener la dirección URL de un sitio de Citrix Receiver para Web existente en el servidor de StoreFront. Para ocuparse de esto, Citrix ADC 11.1 (y versiones posteriores) se pone en contacto con el servidor de StoreFront y enumera todos los almacenes 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 y recurrir a 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 <example.com>, y StoreFront se encuentra en la red privada de la empresa y usa una URL <example.

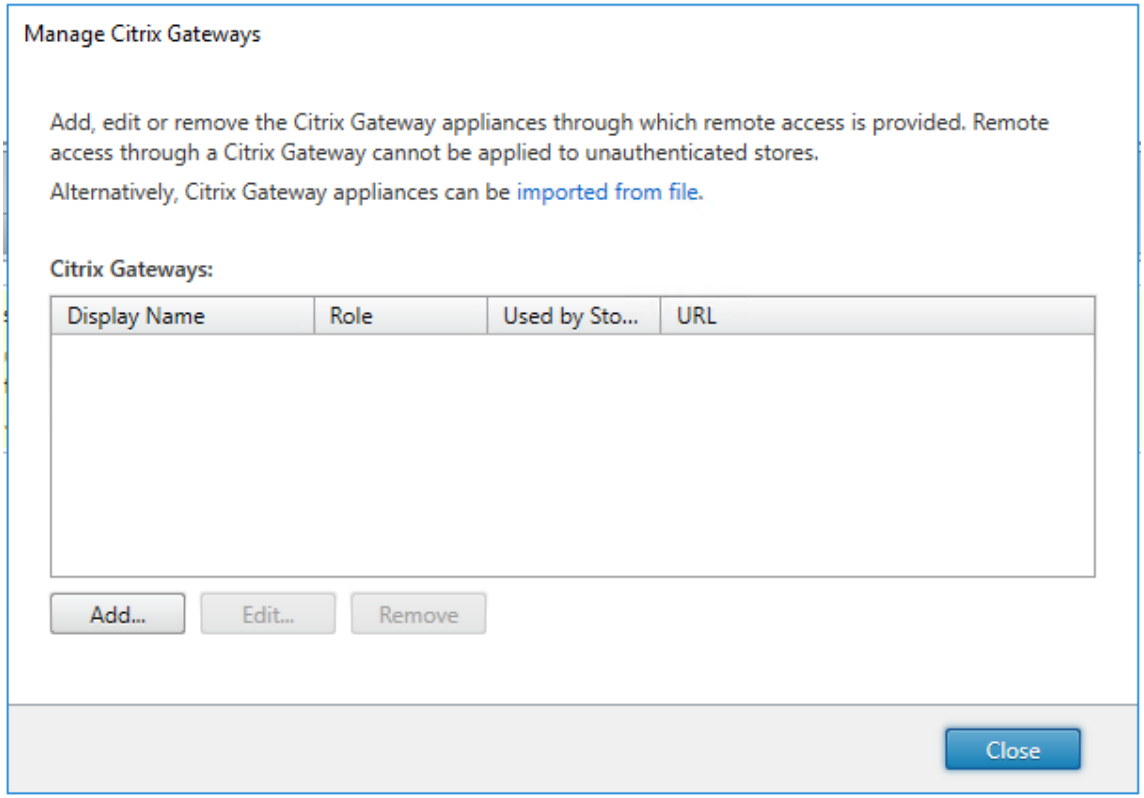
local> puede utilizar una URL de respuesta <example.local> para apuntarla de vuelta al servidor virtual de la puerta de enlace en la DMZ.

Importar un dispositivo Citrix Gateway mediante la consola

Puede importar una o varias configuraciones de servidor virtual de Citrix Gateway mediante el mismo archivo de importación. Si tiene varios servidores virtuales de puerta de enlace de diferentes dispositivos Citrix ADC, debe utilizar varios archivos de importación.

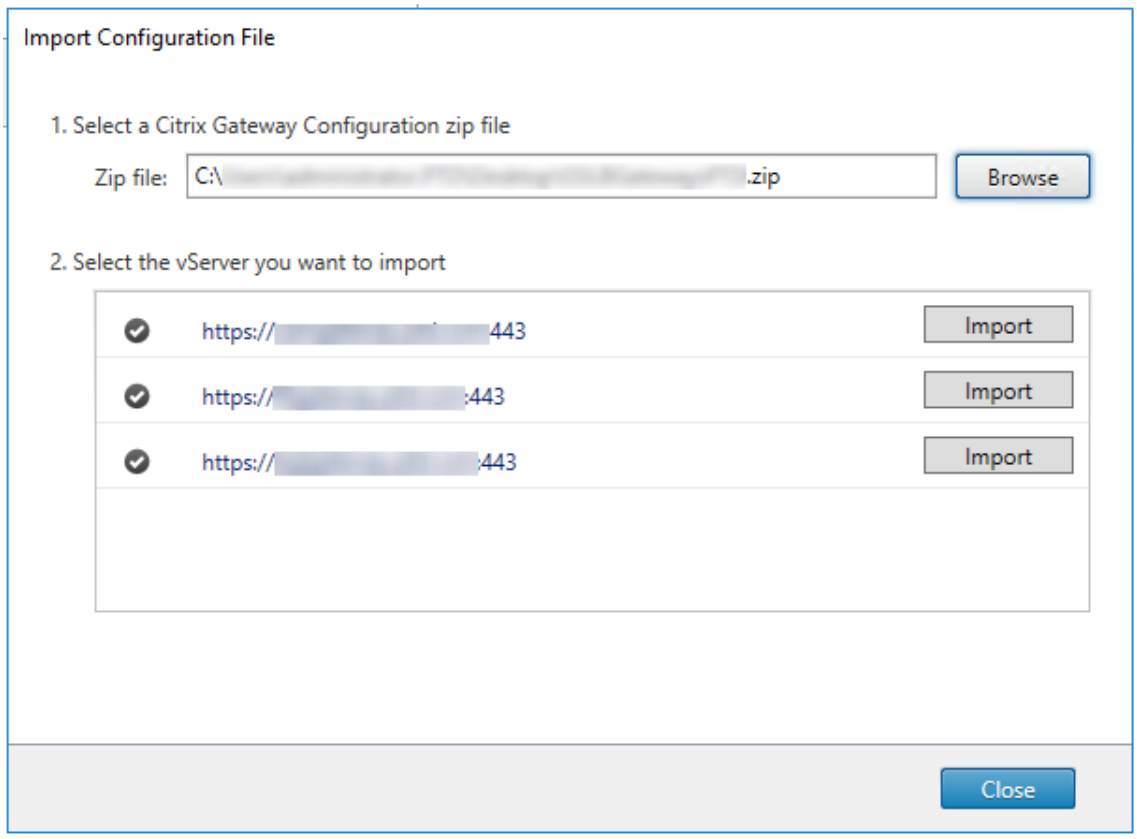
> Importante:
>
> Citrix no admite la modificación manual del archivo de configuración exportado desde Citrix Gateway.

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Citrix Gateway**.
2. En la pantalla Administrar Citrix Gateway, haga clic en el enlace **Importar desde un archivo**.

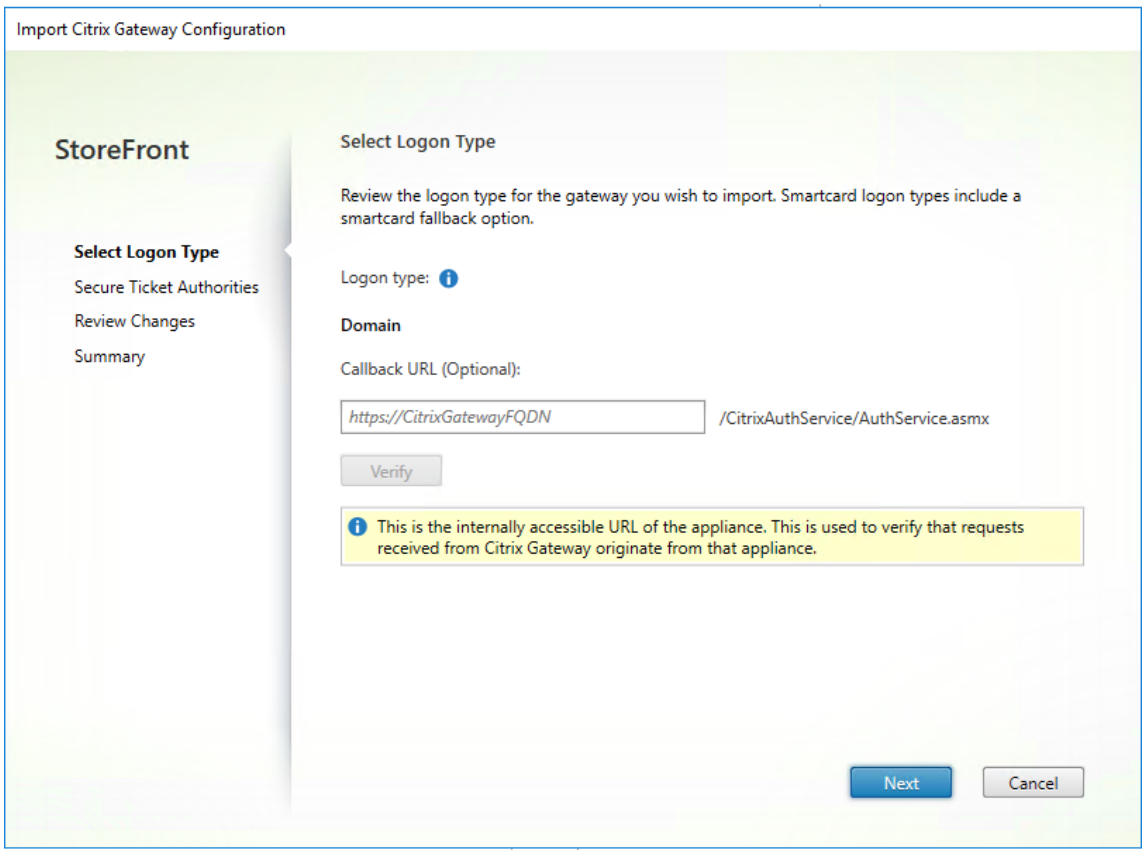


3. Busque el archivo de configuración del servidor virtual de Citrix Gateway.
4. Se muestra una lista de servidores virtuales de puerta de enlace del archivo ZIP seleccionado. Seleccione el servidor virtual de puerta de enlace que quiere importar y haga clic en **Importar**.

Si se repite la importación de un servidor virtual, el botón Importar aparece como botón Actualizar. Si elige **Actualizar**, tiene la opción más adelante de sobrescribir o crear otra 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 Citrix Gateway para los usuarios de la aplicación Citrix Workspace. 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 de StoreFront.

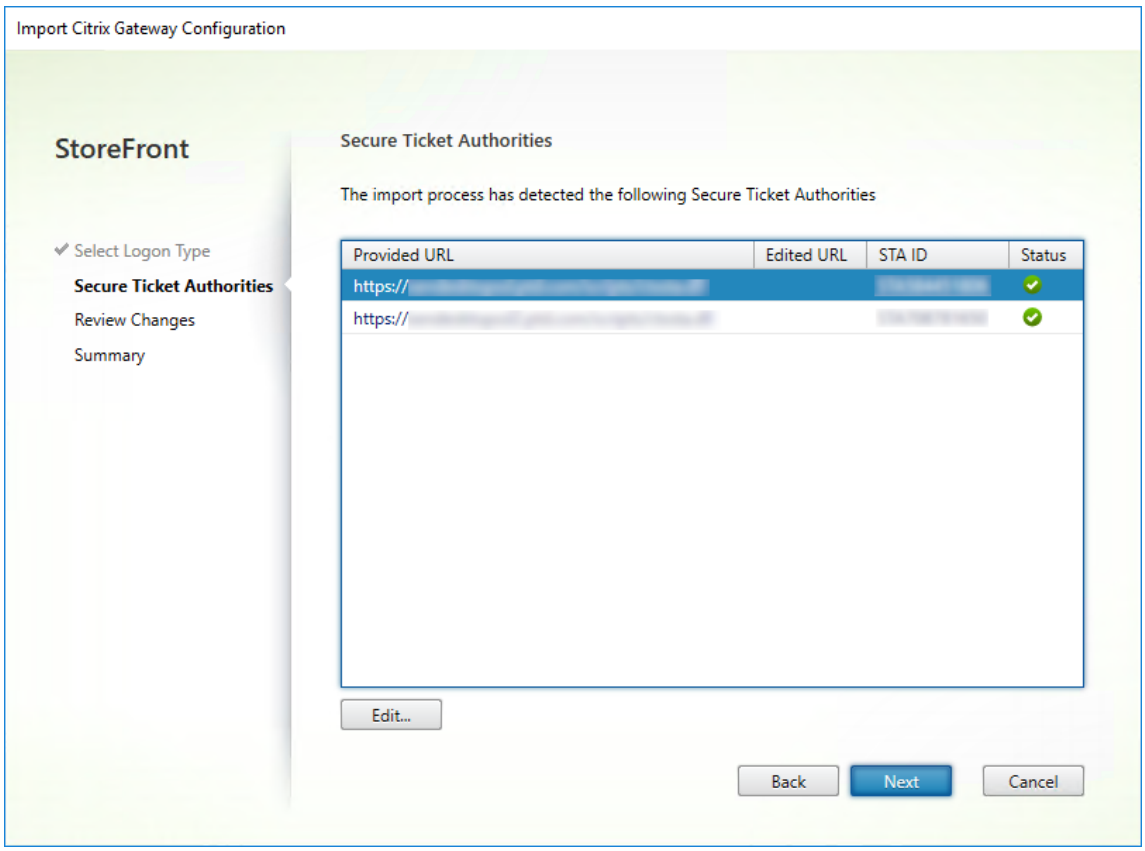


Tipo de inicio de sesión en consola	LogonType en el archivo JSON	URL de respuesta (requerida)
Dominio	Dominio	No
Dominio y token de seguridad	DomainAndRSA	No
Token de seguridad	RSA	Sí
Tarjeta inteligente: Sin alternativa	SmartCard	Sí
Tarjeta inteligente: Dominio	SmartCardDomain	Sí
Tarjeta inteligente: Dominio y token de seguridad	SmartCardDomainAndRSA	Sí
Tarjeta inteligente: Token de seguridad	SmartCardRSA	Sí
Tarjeta inteligente: Autenticación SMS	SmartCardSMS	Sí
Autenticación SMS	SMS	Sí

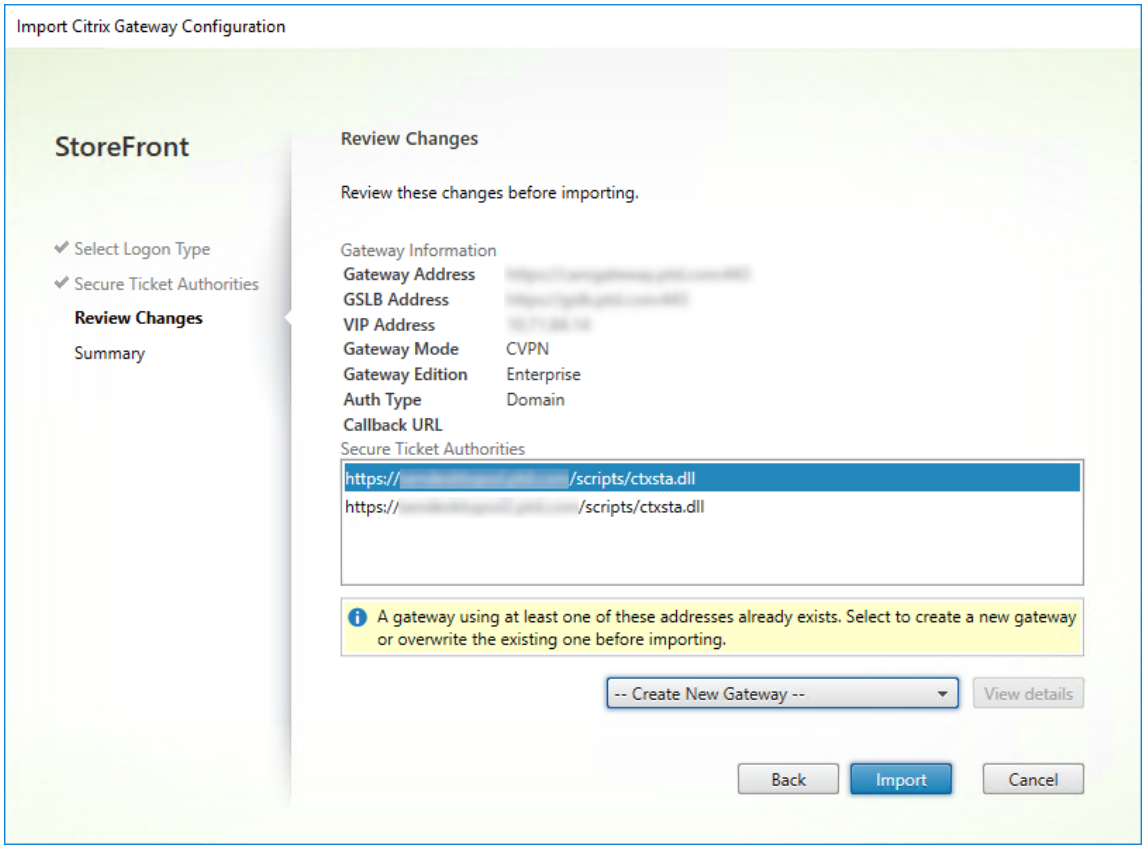
Si se requiere una URL de respuesta, StoreFront rellenará la URL de respuesta en función de la URL de la puerta de enlace encontrada en el archivo ZIP. Se puede cambiar a cualquier dirección URL válida que apunte a la dirección IP virtual de Citrix Gateway. Para las puertas de enlace GSLB, se requieren direcciones URL de respuesta únicas para cada puerta de enlace que importe.

Para utilizar SmartAccess, se necesita una dirección URL de respuesta.

6. Haga clic en **Siguiente**.
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 tíquets STA operativos. La importación no continuará si alguna o varias de las direcciones URL de STA no son válidas.



8. Haga clic en **Siguiente**.
9. Revise los detalles de la importación. Si ya existe una puerta de enlace con la misma combinación de dirección URL y puerto (URL_PuertaDeEnlace: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

Parámetro de la puerta de enlace	Puede actualizarse
Todos los tipos de inicio de sesión	Sí

10. Haga clic en **Importar**. Si el servidor de 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 un almacén es la puerta de enlace a través de la que las aplicaciones Citrix Workspace intentan conectarse a menos que estén configurados para usar una puerta de enlace diferente. Si no hay ninguna puerta de enlace configurada para el almacén, la primera puerta de enlace que se importe desde el archivo ZIP se convertirá en la puerta de enlace predeterminada utilizada por las aplicaciones Citrix Workspace. La importación de puertas de enlace subsiguientes no cambia la puerta de enlace predeterminada que se haya configurado ya para el almacén.

Importar varios dispositivos Citrix Gateway mediante PowerShell

Read-STFNetScalerConfiguration

- Copie el archivo ZIP al escritorio del administrador de StoreFront conectado en ese momento.
- Lea el contenido del ZIP del archivo de configuración de servidor virtual de Citrix Gateway en memoria y consulte las tres puertas de enlace que contiene mediante sus valores de índice.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
```

Consulte los tres objetos de puerta de enlace en memoria que se leyeron desde el paquete de importación ZIP de NetScaler con el cmdlet **Read-STFNetScalerConfiguration**.

```
$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 }
```

Cmdlet Import-STFNetScalerConfiguration sin especificar una dirección URL de respuesta

Copie el archivo ZIP al escritorio del administrador de StoreFront conectado en ese momento. Lea el paquete ZIP importado de configuración de Citrix Gateway en memoria y consulte las tres puertas de enlace que contiene mediante sus valores de índice.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$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.

```
```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
   GatewayIndex 0 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
   GatewayIndex 1 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
   GatewayIndex 2 -Confirm:$False
```
```

Cmdlet Import-STFNetScalerConfiguration especificando su propia dirección URL de respuesta

Importe tres nuevas puertas de enlace en StoreFront con el cmdlet **Import-STFNetScalerConfiguration** y especifique la URL de respuesta que quiera con el parámetro -callbackURL.


```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -
    Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -
    Confirm:$False
```

Cmdlet Import-STFNetScalerConfiguration para anular el método de autenticación almacenado en el archivo de importación y especificar su propia dirección URL de respuesta

Importe tres nuevas puertas de enlace en StoreFront con el cmdlet **Import-STFNetScalerConfiguration** y especifique la URL de respuesta que quiera con el parámetro -callbackURL.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:443" -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:444" -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
    emeagatewaycb.example.com:445" -Confirm:$False
```

Configurar parámetros de conexión de Citrix Gateway

January 6, 2020

Las siguientes tareas permiten actualizar la información de las implementaciones de Citrix Gateway a través de las cuales los usuarios acceden a sus almacenes. Para obtener más información sobre cómo configurar Citrix Gateway para StoreFront, consulte Usar WebFront para la integración con StoreFront.

Si realiza cambios en sus implementaciones de Citrix Gateway, asegúrese de que los usuarios que acceden a los almacenes a través de estas implementaciones actualicen la aplicación Citrix Workspace con la información de conexión modificada. Cuando se configura un sitio de Citrix Receiver para Web para un almacén, los usuarios pueden obtener un archivo de aprovisionamiento actualizado de la aplicación Citrix Workspace del sitio. De lo contrario, puede exportar un archivo de aprovisionamiento para el almacén y hacer que este archivo esté disponible para sus usuarios.

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

Cambiar parámetros generales de Citrix Gateway

Utilice la tarea Cambiar parámetros generales para modificar los nombres de las implementaciones de Citrix 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 Citrix 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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront y haga clic en Administrar Citrix Gateway.
3. Especifique un nombre para la implementación de Citrix Gateway que ayude a los usuarios a identificarla.

   Los usuarios verán el nombre simplificado que especifique en la aplicación Citrix Workspace, de modo que debe incluir la información relevante en el nombre para ayudarlos a decidir si utilizar esa implementación o no. Por ejemplo: puede incluir la ubicación geográfica en los nombres simplificados para las implementaciones de Citrix 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) de la implementación de StoreFront debe ser único

y diferente del FQDN del servidor virtual de Citrix Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de Citrix Gateway.

5. Si su implementación de Access Gateway 5.0 se está ejecutando, continúe en el paso 7. De lo contrario, especifique la dirección IP de subred del dispositivo Citrix Gateway, si es necesario.

   La dirección de subred es la dirección IP que Citrix 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 Citrix 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 tiene Citrix Gateway, seleccione en la lista Tipo de inicio de sesión el método de autenticación configurado en el dispositivo para los usuarios de la aplicación Citrix Workspace.

   La información que proporcione sobre la configuración de su dispositivo Citrix Gateway se agrega al archivo de aprovisionamiento para el almacén. Eso permite que la aplicación Citrix Workspace 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 Citrix Gateway o un único dispositivo Access Gateway 5.0, complete la dirección URL del servicio de autenticación de Citrix 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 Citrix Gateway para verificar que las solicitudes recibidas desde Citrix Gateway provienen de ese dispositivo.

Administrar 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.

Habilitar 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 los almacenes.

Administrar Secure Ticket Authorities

Utilice la tarea Secure Ticket Authority para actualizar la lista de Secure Ticket Authorities (STA) de los cuales StoreFront obtiene tíquets de sesión de usuario y para configurar la fiabilidad de la sesión. El STA está alojado en servidores Citrix Virtual Apps and Desktops. Emite tíquets de sesión en respuesta a las solicitudes de conexión. Esos tíquets de sesión forman la base de la autenticación y la autorización para acceder a los recursos de Citrix Virtual Apps and Desktops.

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 Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione una implementación de Citrix Gateway. En el panel Acciones, haga clic en Administrar Citrix 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 tíquets de sesión de ese STA.
4. Si quiere que Citrix Virtual Apps and Desktops mantenga abiertas las sesiones desconectadas mientras la aplicación Citrix Workspace intenta volver a conectarse automáticamente, marque la casilla Habilitar fiabilidad de la sesión. Si configuró varios STA y quiere asegurarse de que la fiabilidad de la sesión esté siempre disponible, seleccione la casilla Solicitar tíquets de dos STA, si están disponibles.

Cuando la casilla Solicitar tíquets de dos STA, si están disponibles está seleccionada, StoreFront obtiene tíquets 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 Citrix Gateway

En el panel **Acciones**, utilice la tarea Quitar en **Administrar Citrix Gateway** para eliminar de StoreFront la información de una implementación de Citrix Gateway. Una vez que se haya quitado una implementación de Citrix Gateway, los usuarios ya no pueden acceder a los almacenes a través de esa implementación.

Equilibrio de carga con dispositivos Citrix ADC

January 6, 2020

En este artículo se ofrecen instrucciones acerca de cómo implementar un grupo de servidores de StoreFront que contengan como mínimo dos servidores de StoreFront en toda la configuración activa de equilibrio de carga. En el artículo se ofrece información detallada acerca de cómo configurar un dispositivo Citrix ADC para equilibrar la carga de solicitudes entrantes de la aplicación Citrix Workspace y Citrix Receiver para Web entre los nodos de StoreFront del grupo de servidores. En este artículo también se muestra cómo configurar un monitor de StoreFront para usarlo con un dispositivo Citrix ADC.

Los ejemplos de esta sección se han probado en el siguiente entorno:

- Cuatro nodos de StoreFront 3.x con Windows Server 2012 R2 en un solo grupo de servidores.
- Un equilibrador de carga de un dispositivo Citrix ADC 12.1 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 con Windows 10 con la aplicación Citrix Workspace instalada.

Requisitos de certificado de servidor para la implementación con equilibrio de carga, si quiere utilizar HTTPS

Revise la sección Planificar el 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.

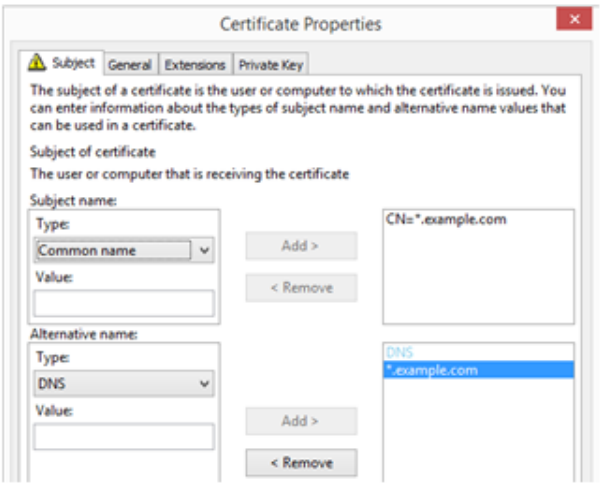
- **Opción 1:** Usar un certificado comodín **.ejemplo.com* en el servidor virtual de equilibrio de carga del dispositivo Citrix ADC y en los nodos del grupo de servidores de StoreFront. Esto simplifica la configuración y permite agregar más servidores de StoreFront en el futuro, sin la necesidad de reemplazar el certificado.
- **Opción 2:** Usar un certificado que incluya nombres alternativos de sujeto (SAN) en el servidor virtual de equilibrio de carga del dispositivo Citrix ADC y en los nodos del grupo de servidores de StoreFront. Los nombres SAN adicionales que contenga el certificado que coincidan con todos los nombres de dominio completos (FQDN) de servidor de StoreFront son opcionales aunque se recomiendan, ya que permiten una mayor flexibilidad en la implementación de StoreFront. Incluir un nombre SAN para la detección basada en correo electrónico como, por ejemplo, discoverReceiver.ejemplo.com.

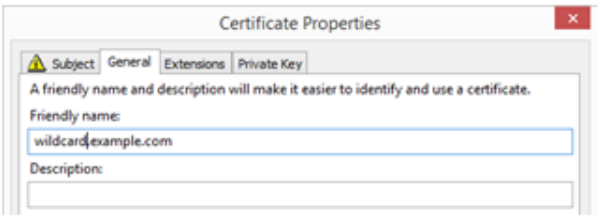
Para obtener más información sobre la configuración de detección basada en correo electrónico, consulte http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/.

> **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 del dispositivo Citrix ADC y otro distinto en los nodos del grupo de servidores de StoreFront. Ambos certificados deben incluir nombres alternativos de sujeto.

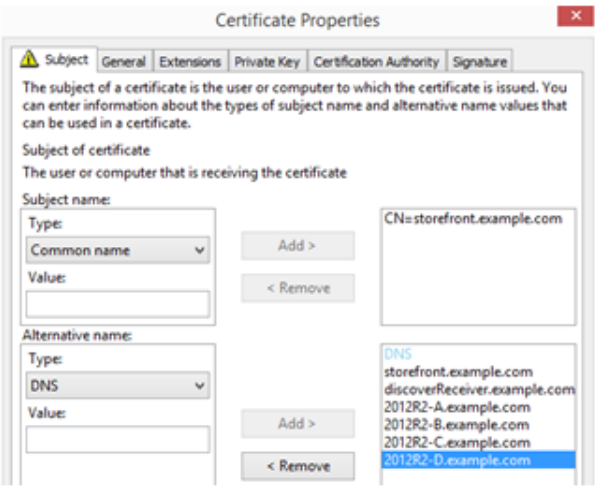
Example Web server certificates

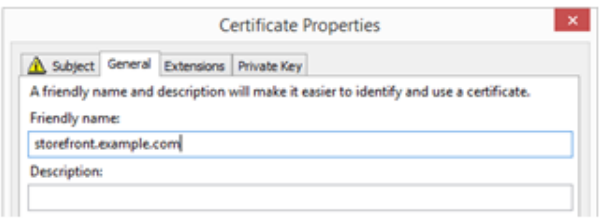
Option 1: Wildcard certificate



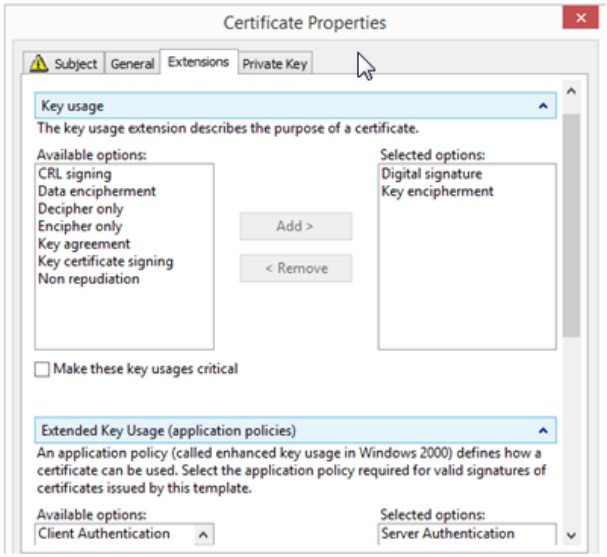


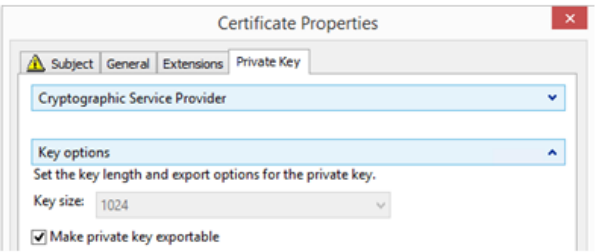
Option 2: SAN certificate with every StoreFront server





Common Properties





Crear un certificado de servidor para el equilibrador de carga del dispositivo Citrix ADC y todos los servidores de StoreFront

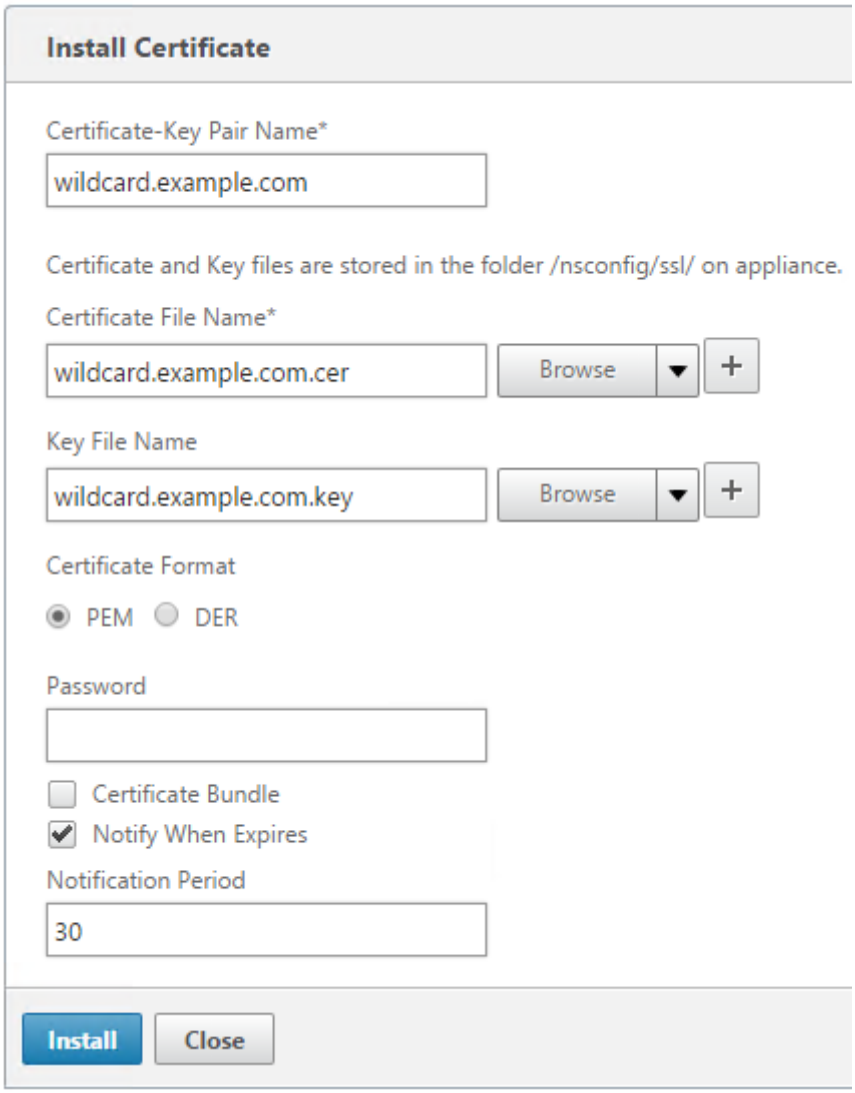
Importar un certificado emitido por una entidad de certificación Windows en un dispositivo Citrix ADC

- WinSCP es una útil herramienta externa y gratuita para trasladar archivos de una máquina con Windows al sistema de archivos de un dispositivo Citrix ADC. Copie los certificados que quiere importar en la carpeta */nsconfig/ssl/* del sistema de archivos del dispositivo Citrix ADC.
- También puede usar las herramientas de OpenSSL en el dispositivo Citrix ADC para extraer el certificado y la clave de un archivo *PKCS12/PFX* y así crear dos archivos X.509 separados (.CER y .KEY) en formato PEM que Citrix ADC puede utilizar.

1. Copie el archivo PFX en */nsconfig/ssl*, en el dispositivo Citrix ADC o en VPX.
2. Abra la interfaz de línea de comandos (CLI) del dispositivo Citrix ADC.
3. Escriba **Shell** para salir de la interfaz de línea de comandos del dispositivo Citrix ADC y pasar al shell de FreeBSD.
4. Cambie el directorio con `cd /nsconfig/ssl/`.
5. Ejecute `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` e introduzca la contraseña de PFX cuando se le pida.
6. Ejecute `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key` y escriba la contraseña del archivo PFX cuando se le solicite y, a continuación, establezca la frase de contraseña con formato PEM de clave privada 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 del dispositivo Citrix ADC.

Configurar el certificado de servidor en el dispositivo Citrix ADC después de importarlo

1. Inicie sesión en la GUI de administración de dispositivos Citrix ADC.
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 del dispositivo Citrix ADC, en /nsconfig/ssl/.
    - Seleccione, en la misma ubicación, el archivo .key que contiene la clave privada.



Crear registros DNS para el equilibrador de carga del grupo de servidores de 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 de StoreFront mediante el equilibrador de carga del dispositivo Citrix ADC.

Ejemplo: `storefront.example.com` recurre a la dirección IP virtual (VIP) del servidor virtual del equilibrio de carga.

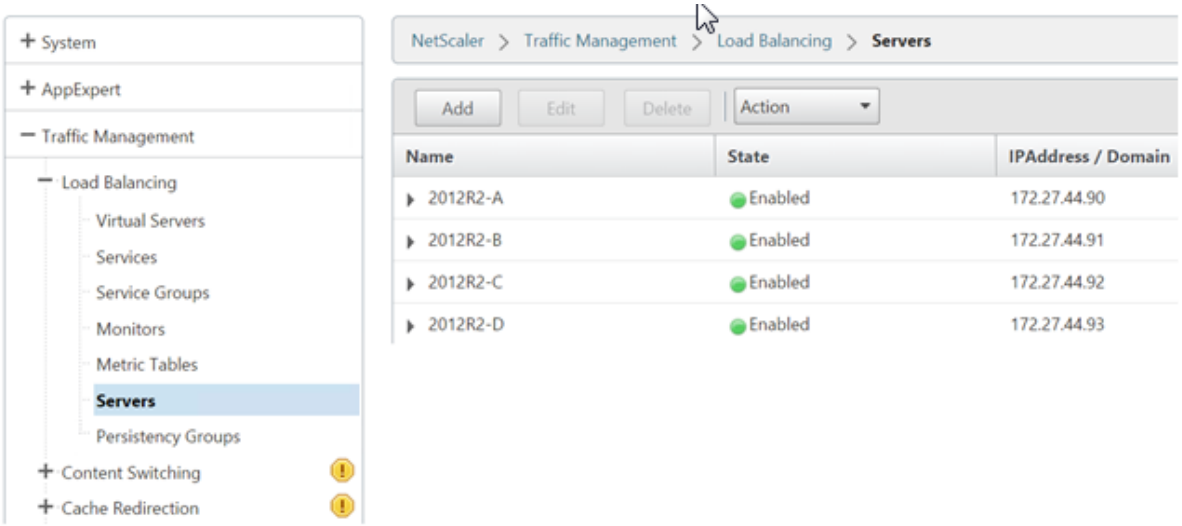
Caso 1: Las conexiones HTTPS 443 seguras de extremo a extremo entre el cliente y el equilibrador de carga del dispositivo Citrix ADC, y entre el equilibrador de carga y varios servidores de StoreFront 3.x

En este caso, se usa un monitor de StoreFront modificado, a través del puerto 443.

Agregar nodos de servidor de StoreFront individuales al equilibrador de carga del dispositivo Citrix ADC

1. Inicie sesión en la GUI de administración de dispositivos Citrix ADC.
2. Seleccione **Traffic Management > Load Balancing > Servers > Add** y agregue cada uno de los cuatro nodos de StoreFront cuyas cargas quiere equilibrar.

   Ejemplo = 4 nodos de StoreFront 2012R2 denominados 2012R2-A, -B, -C y -D.
3. Use una configuración de servidor basada en IP y especifique la dirección IP del servidor de cada nodo de StoreFront.

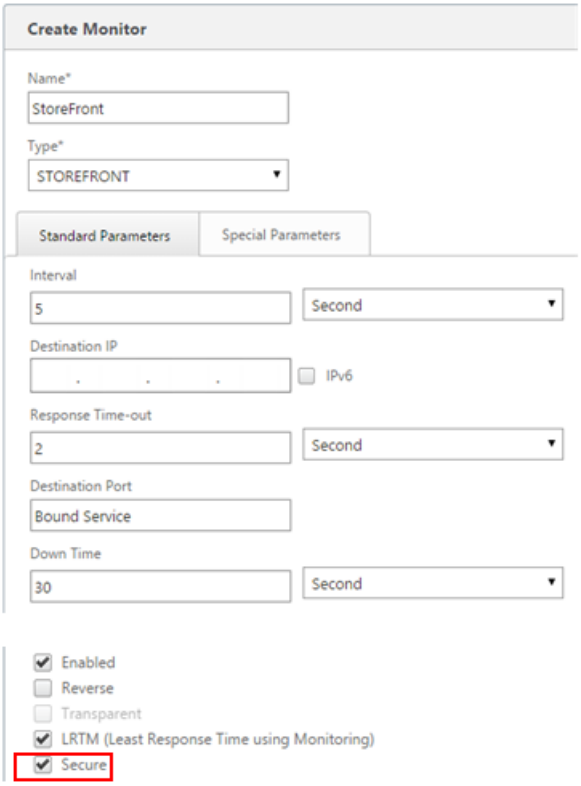


Definir un monitor de StoreFront para consultar el estado de todos los nodos de StoreFront en el grupo de servidores

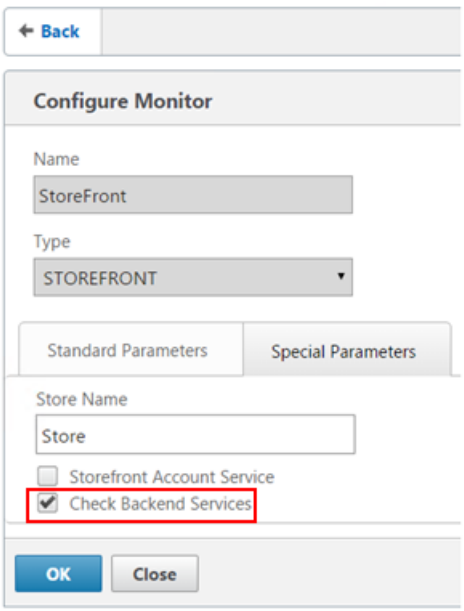
1. Inicie sesión en la GUI de administración de Citrix ADC.
2. Seleccione **Traffic Management > Load Balancing > Monitors > Add**, agregue un nuevo monitor llamado *StoreFront* y acepte todos los parámetros predeterminados.
3. En el menú desplegable **Type**, seleccione **StoreFront**.
4. Si utiliza conexiones HTTPS entre el servidor virtual de equilibrio de carga y StoreFront, debe seleccionar la opción **Secure**; si no las utiliza, deje esta opción sin seleccionar.

5. En la ficha **Special Parameters**, escriba el nombre del almacén en **Store Name**.
6. En la ficha **Special Parameters**, seleccione la opción **Check Backend Services**. Esta opción permite supervisar los servicios que se ejecuten en el servidor de StoreFront. Los servicios de StoreFront se supervisan por sondeo de un servicio Windows que se ejecuta en el servidor de StoreFront, el cual devuelve el estado de los siguientes servicios:
   - W3SVC (IIS)
   - Servicio WAS (Windows Process Activation Service)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService

Standard Parameters Tab

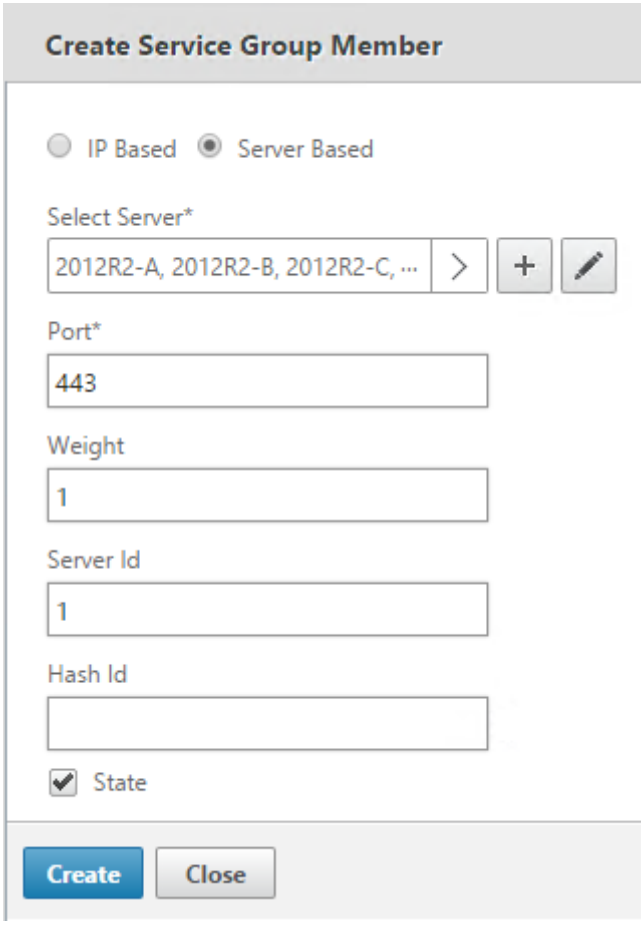


Special Parameters Tab

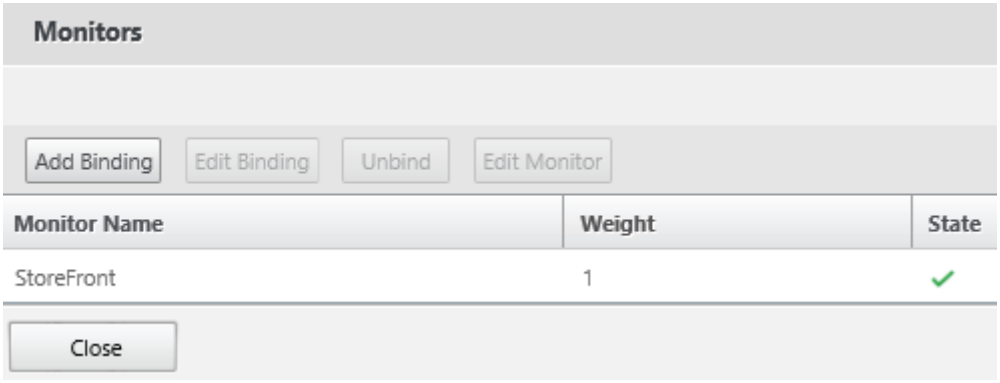


Crear un grupo de servicios HTTPS 443 que contenga todos los servidores de StoreFront

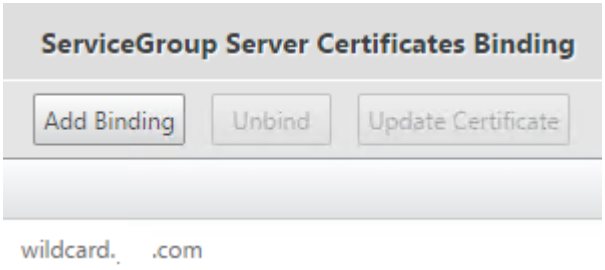
1. En el grupo de servicios, seleccione la opción **Members** en el lado derecho y agregue todos los nodos de servidor de StoreFront que ha definido previamente en el apartado de servidores.
2. Configure el puerto TLS y adjudique a cada nodo un ID de servidor único a media que los agrega.



3. En la ficha **Monitors**, seleccione el monitor de StoreFront que ha creado anteriormente.

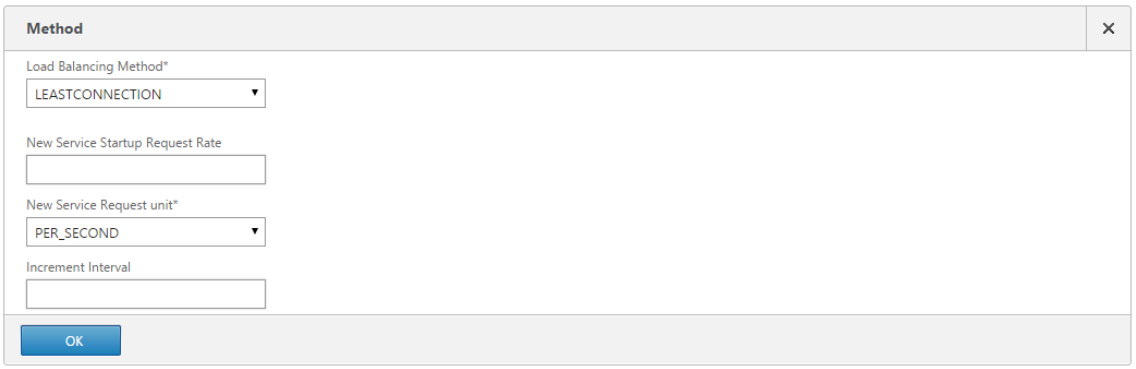


4. En la ficha **Certificates**, enlace el certificado de servidor que ha importado anteriormente.
5. Enlace el certificado de CA usado para firmar el certificado de servidor que ha importado antes, así como cualquier otra entidad de certificación (CA) que pueda formar parte de la cadena de confianza de la infraestructura de clave pública (PKI).

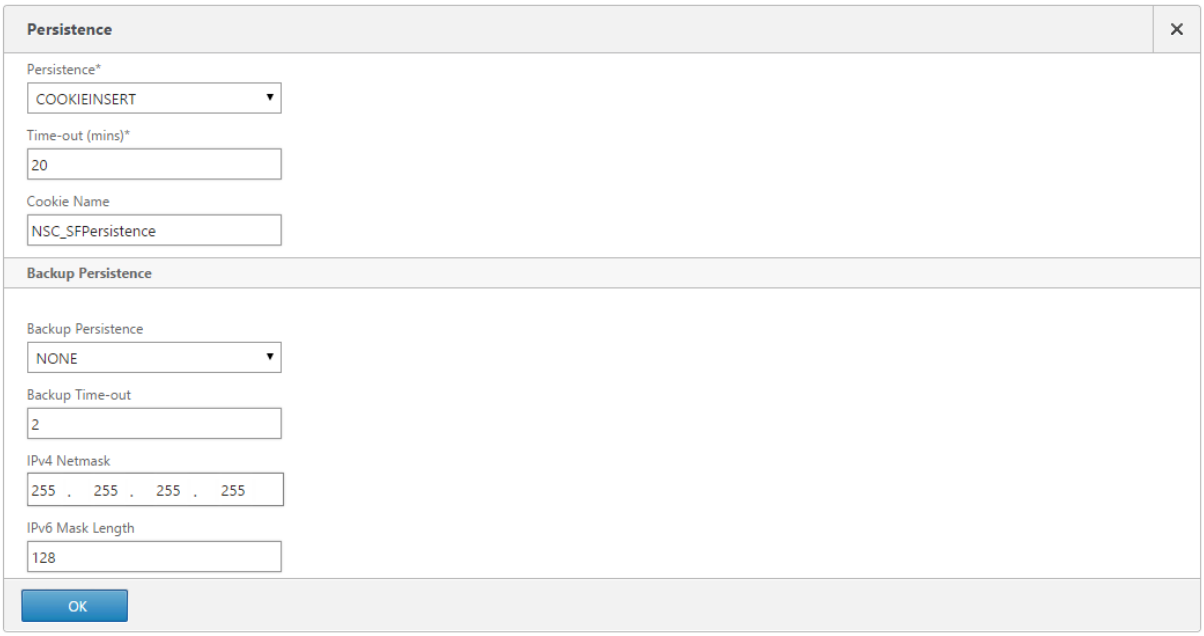


Crear un servidor virtual de equilibrio de carga para el tráfico del usuario

1. Inicie sesión en la GUI de administración de dispositivos Citrix ADC.
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 hace que sea fácil de identificar en las trazas de Fiddler durante la depuración.
8. Establezca la persistencia de reserva en **NONE**.



Caso 2: Terminación HTTPS. Comunicación HTTPS 443 entre el cliente y el equilibrador de carga de Citrix ADC, y conexiones HTTP 80 entre el equilibrador de carga y los servidores de StoreFront 3.x detrás de él

En este caso, se usa el monitor predeterminado de StoreFront a través del puerto 8000.

Agregar servidores individuales de StoreFront al equilibrador de carga de Citrix ADC

1. Inicie sesión en la GUI de administración de Citrix ADC.
2. Seleccione **Traffic Management > Load Balancing > Servers > Add** y agregue cada uno de los cuatro nodos de StoreFront cuyas cargas quiere equilibrar. Ejemplo = 4 servidores de StoreFront 2012R2 denominados 2012R2-A, -B, -C y -D. 3.
3. Use una configuración de servidor basada en IP y especifique la dirección IP del servidor de cada servidor de StoreFront.

Definir un monitor de StoreFront HTTP 8000 para consultar el estado de todos los servidores de StoreFront en el grupo de servidores

1. Inicie sesión en la GUI de administración de Citrix ADC.
2. Seleccione **Traffic Management > Monitors > Add** y agregue un nuevo monitor llamado Store-Front.
3. Agregue un nombre para el nuevo monitor y acepte los valores predeterminados.
4. En la lista **Type**, seleccione **StoreFront**.
5. En la ficha **Special Parameters**, escriba el nombre del almacén en **Store Name**.

6. Escriba 8000 en **Destination Port**. Esto coincide con la instancia de monitor predeterminada que se crea en cada servidor de StoreFront.
7. En la ficha **Special Parameters**, seleccione la opción **Check Backend Services**. Esta opción permite supervisar los servicios que se ejecuten en el servidor de StoreFront. Los servicios de StoreFront se supervisan por sondeo de un servicio Windows que se ejecuta en el servidor de StoreFront, el cual devuelve el estado de todos los servicios de StoreFront en ejecución.

Crear un grupo de servicios HTTP 80 que contenga todos los servidores de StoreFront

1. En el grupo de servicios, seleccione la opción **Members** en el lado derecho y agregue todos los nodos de servidor de 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 a medida que lo agrega.
3. En la ficha **Monitors**, seleccione el monitor de StoreFront que ha creado anteriormente.

Crear 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 usa la persistencia.

5. 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**.
6. Dé un nombre a la cookie. Por ejemplo, **NSC_SFPersistence**, ya que esto hace que sea fácil de identificar en las trazas de
   Fiddler durante la depuración.

7. Establezca la persistencia de reserva en **NONE**.

Crear un servidor virtual de equilibrio de carga para la sincronización de suscripciones entre grupos de servidores

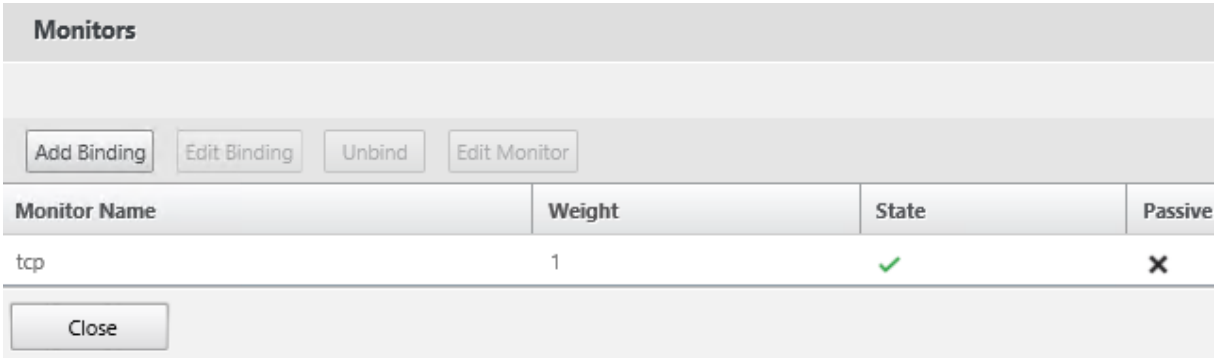
Entre los aspectos a tener en cuanta antes de crear un servidor virtual de equilibrio de carga, se incluyen los siguientes:

- **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 de 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 de 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 ofrecer una alta disponibilidad en este servicio, cree un segundo servidor virtual en cada dispositivo Citrix ADC de la implementación. De esta manera, equilibrará la carga en el puerto TCP 808 proveniente de cada grupo de servidores de 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.

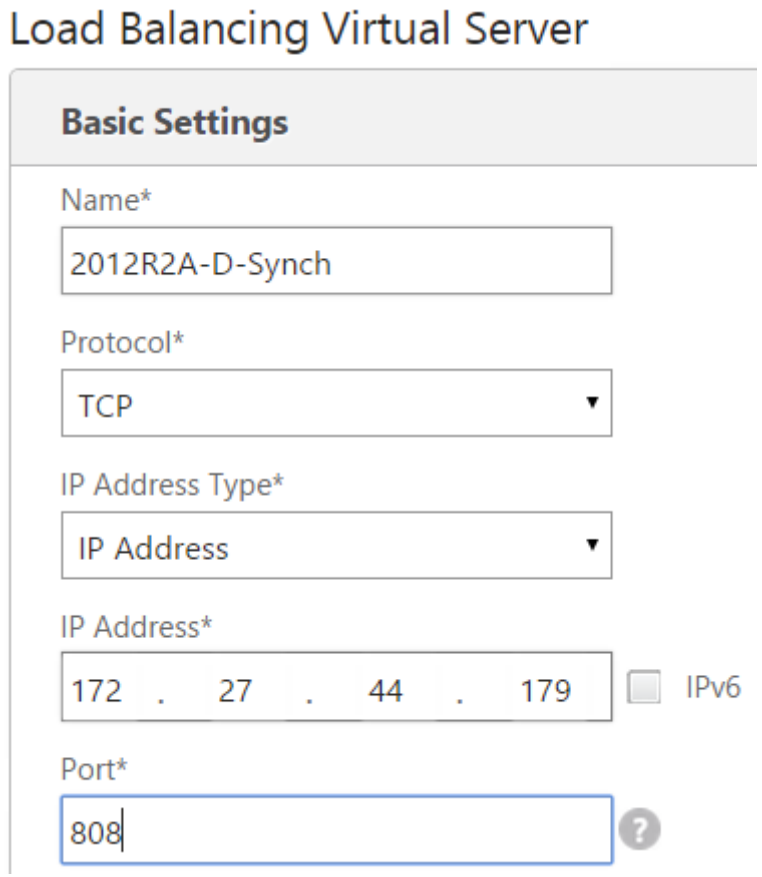
Configurar un grupo de servicios para la sincronización de suscripciones

1. Inicie sesión en la GUI de administración de dispositivos Citrix ADC.
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 de StoreFront que ha definido previamente en el apartado de servidores.
5. En la ficha **Monitors**, seleccione el monitor de TCP.



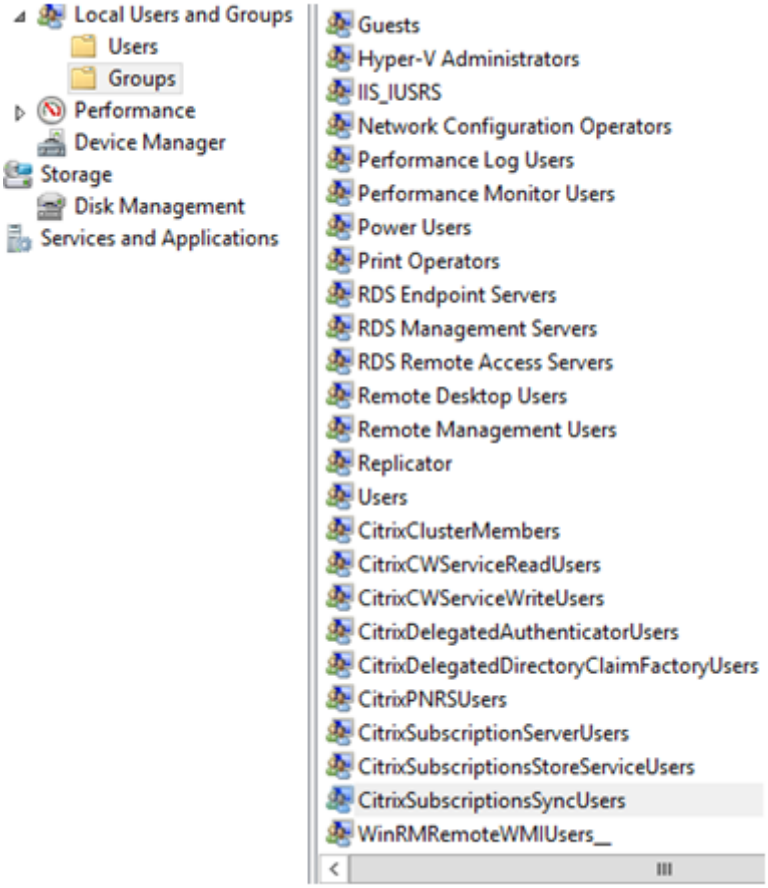
Crear un servidor virtual de equilibrio de carga para la sincronización de suscripciones entre grupos de servidores

1. Inicie sesión en la GUI de administración de dispositivos Citrix ADC.
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

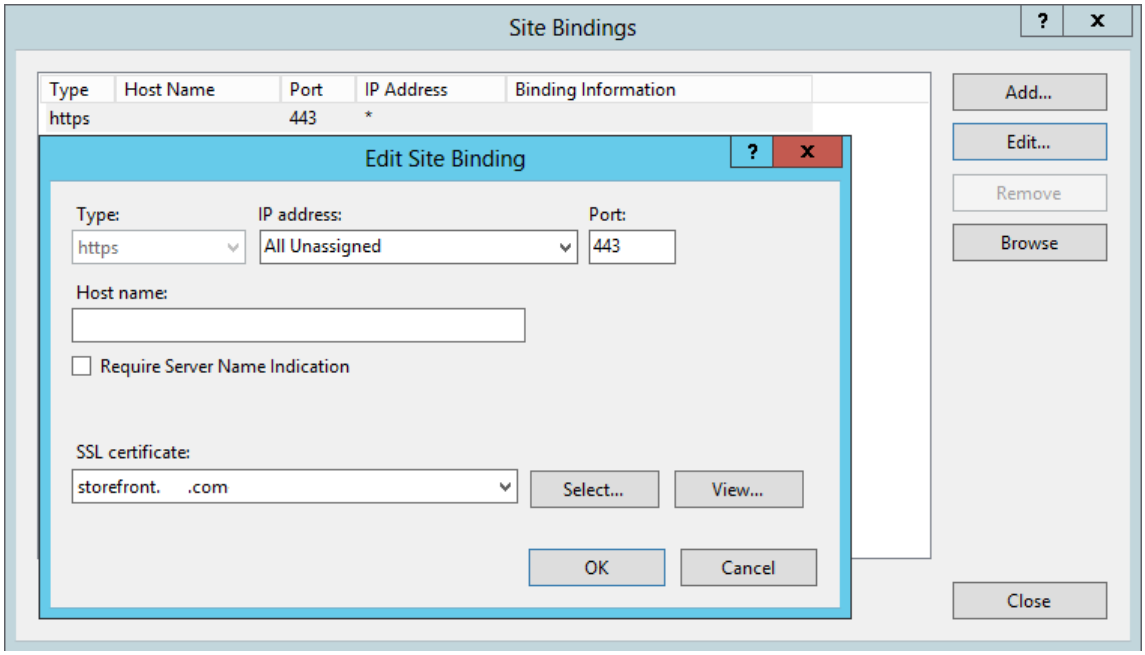
Para que el **servidor de StoreFront A** en la **Ubicación A** solicite y extraiga datos de suscripción del **servidor B** en otra ubicación, el servidor A debe ser miembro del grupo de seguridad local **CitrixSubscriptionsSyncUsers** del servidor B. El grupo local **CitrixSubscriptionsSyncUsers** contiene una lista de control de acceso de todos los servidores de 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.



Caso 1: Configurar el grupo de servidores de StoreFront mediante HTTPS entre Citrix ADC y StoreFront

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 equilibrio de carga del dispositivo Citrix ADC.
2. Cree un enlace HTTPS en IIS en cada nodo de StoreFront y, a continuación, vincúlelo al certifi-

cado importado anteriormente.

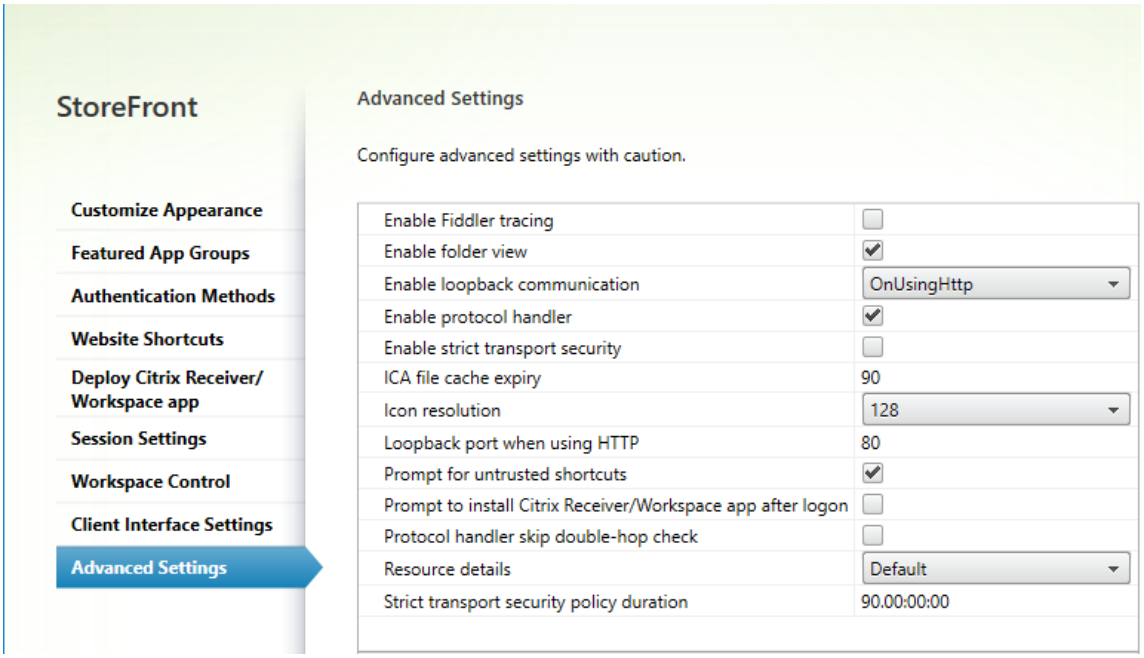


3. Si utiliza HTTPS entre el equilibrador de carga de Citrix ADC y StoreFront, debe usar un certificado que contenga el FQDN de equilibrio de carga como un nombre común (CN) o como un nombre alternativo de sujeto (SAN).

   Consulte Crear un certificado de servidor para el equilibrador de carga del dispositivo Citrix ADC y los servidores de StoreFront.

Caso 2: Configurar el grupo de servidores de StoreFront mediante HTTP entre Citrix ADC y StoreFront

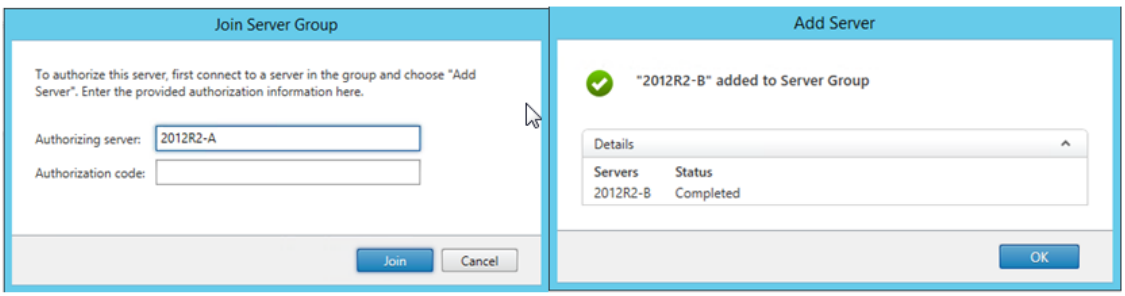
1. Quite el enlace HTTPS en IIS de cada nodo de StoreFront si ya existe.
2. El enlace HTTP debe estar presente en IIS y configurado para usar el puerto 80.
3. Configure los parámetros de bucle invertido en Receiver para Web como **OnUsingHTTP** y puerto **80**. Este paso es esencial para garantizar que la detección de clientes entre la aplicación Citrix Workspace nativa y Receiver para Web se realice correctamente.



Pasos comunes a los casos 1 y 2

1. Instale StoreFront en cada nodo del grupo de servidores.
2. 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. Esto debe ser siempre `https://storefrontlb.domain.com` tanto para el caso 1 como para el caso 2, y debe coincidir con el FQDN del servidor virtual de equilibrio de carga de Citrix ADC.

   Consulte la Crear un certificado de servidor para el equilibrador de carga del dispositivo Citrix ADC y los servidores de StoreFront.
3. Una vez que haya completado la configuración inicial de StoreFront, incorpore cada nodo (uno a uno) al grupo de servidores mediante el nodo principal.
4. Seleccione **Server Group > Add Server > Copy the Authorization Code** en el servidor que se une al grupo.



5. Propague la configuración desde el nodo principal a todos los demás nodos del grupo de servidores.
6. 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 de Windows en los que se basa StoreFront para el funcionamiento correcto, utilice el servicio Windows **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 de StoreFront se determine de forma externa con la ayuda de otros componentes de Citrix como, por ejemplo, un dispositivo Citrix ADC. 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 cada implementación de StoreFront.

Para realizar cambios en el monitor predeterminado existente (como cambiar el protocolo y el puerto a HTTPS 443), utilice los 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

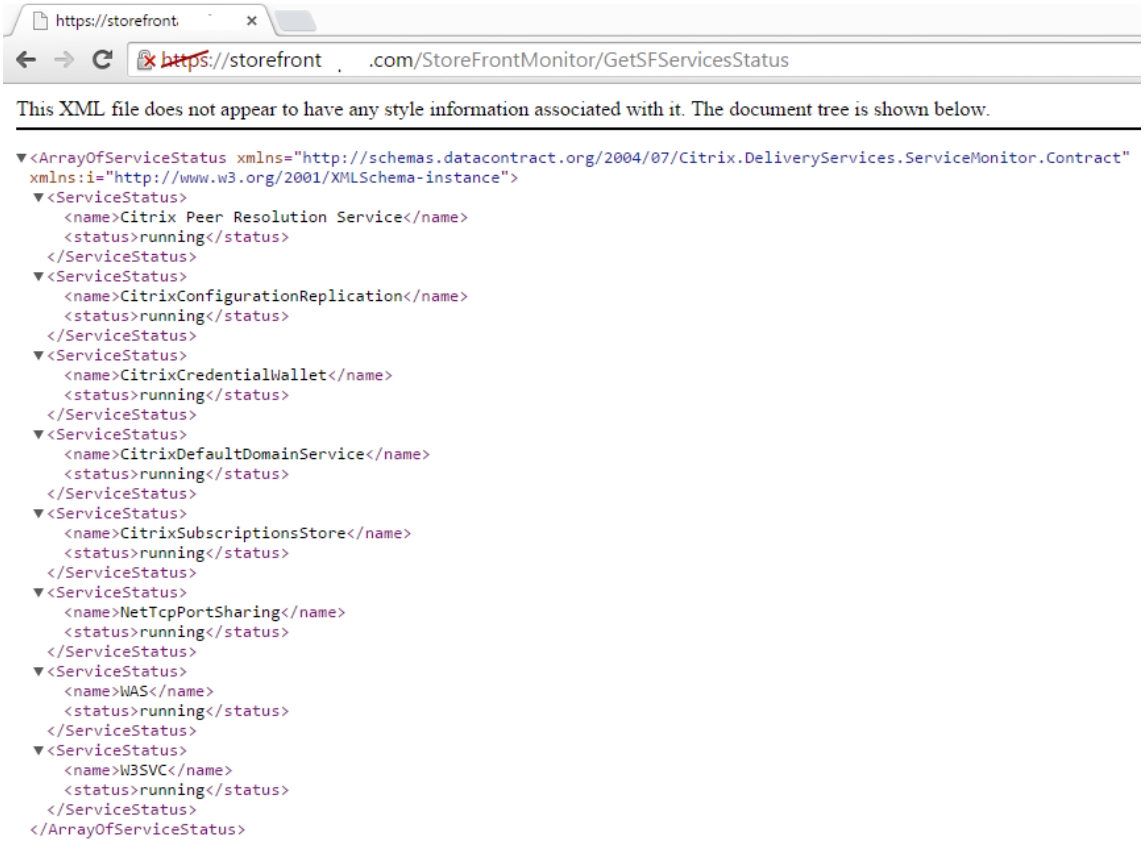
1. Abra el entorno Integrated Scripting Environment (ISE) de PowerShell en el servidor de StoreFront principal y ejecute los comandos siguientes para cambiar el monitor predeterminado a HTTPS 443.

```
$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 de StoreFront.
3. Para realizar una prueba rápida en el nuevo monitor, introduzca la URL siguiente en el explorador web presente en el servidor de StoreFront, o en cualquier otra máquina con acceso de

red al servidor de StoreFront. El explorador debería devolver un resumen XML del estado de cada servicio de StoreFront.

`https://<loadbalancingFQDN>:443/StoreFrontMonitor/GetSFServicesStatus`

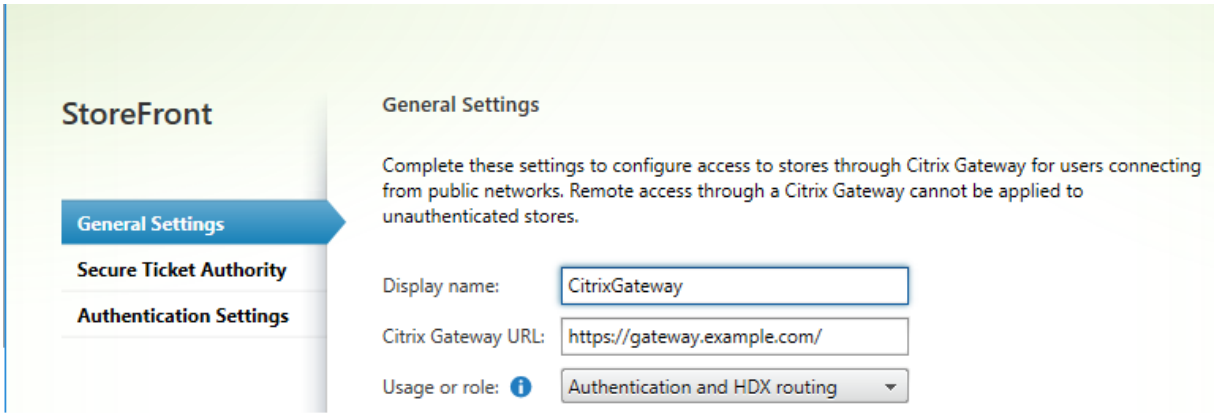


Citrix Gateway y servidores virtuales de equilibrio de carga en el mismo dispositivo Citrix ADC

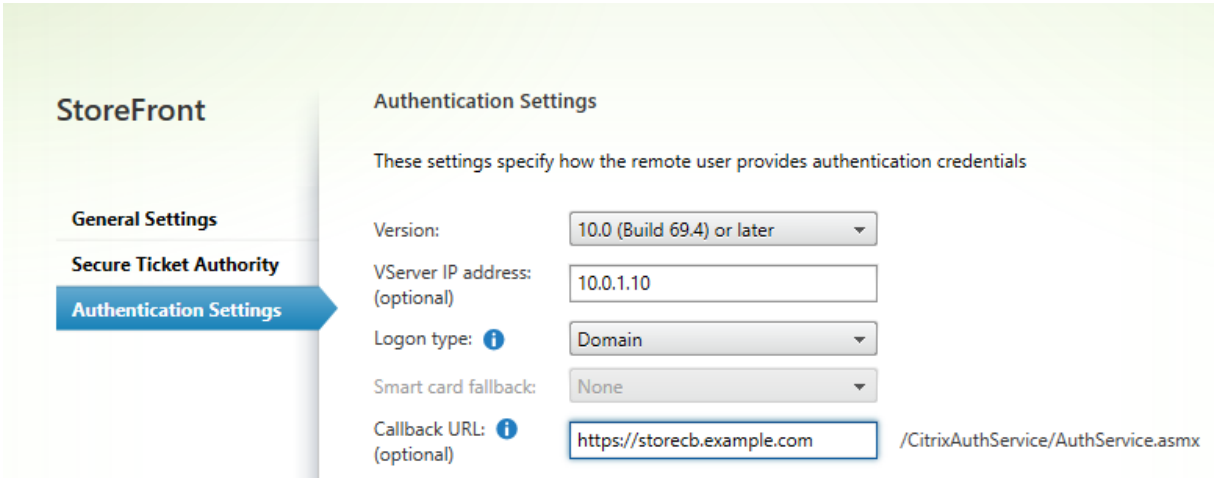
Si ha configurado el servidor virtual de Citrix Gateway y el servidor virtual de equilibrio de carga en el mismo dispositivo Citrix ADC, los usuarios del dominio interno pueden tener problemas al intentar acceder directamente a la URL base del host StoreFront con carga equilibrada en lugar de pasar por el servidor virtual de Citrix Gateway.

En este caso, StoreFront asume que el usuario final ya se ha autenticado en el dispositivo Citrix Gateway, ya que StoreFront correlaciona la dirección IP de origen del usuario entrante con la dirección IP de subred (SNIP) de Citrix Gateway. Por eso, StoreFront intenta usar el protocolo AGBasic para realizar la autenticación silenciosa de Citrix 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 o introduzca una dirección IP virtual, de modo que se use la autenticación con nombre de usuario y contraseña en lugar del protocolo de inicio de sesión AGBasic.

Configurar un dispositivo Citrix Gateway en el grupo de servidores de StoreFront



Introduzca la dirección VIP de Citrix Gateway VIP en el campo de dirección IP del servidor virtual. NO utilice la dirección SNIP para Citrix Gateway si el servidor virtual de equilibrio de carga reside en el mismo dispositivo Citrix ADC.



Opciones de bucle invertido al equilibrar la carga de un grupo de servidores de StoreFront mediante un dispositivo Citrix ADC

Puede definir opciones de bucle con PowerShell.

Ejemplo de archivo web.config de Receiver para Web

```
<communication attempts="2" timeout="00:01:00" loopback="On"
   loopbackPortUsingHttp="80">
```


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
On: 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 utilizar si se utiliza el equilibrador de carga de terminación de TLS.
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 TLS. La comunicación entre el equilibrador de carga y los servidores de 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**.

Configurar dos direcciones URL para un mismo dispositivo Citrix Gateway

January 31, 2020

En StoreFront, puede agregar una dirección de URL de Citrix Gateway desde la consola de administración de StoreFront, con la opción **Administrar Citrix Gateway > Agregar** o **Modificar**. También es posible agregar una URL de Citrix Gateway pública y una URL de equilibrio de carga global de servidores (GSLB) en **Administrar Citrix 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 en-

lace. Esta funcionalidad simplifica la administración de Citrix Gateway en StoreFront en los siguientes casos de uso:

1. **GSLB y varios dispositivos Citrix Gateway**. Use GSLB y varios dispositivos Citrix 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. **Un único dispositivo Citrix Gateway con una URL pública o privada**. Use el mismo dispositivo Citrix Gateway para el acceso externo mediante una URL pública, y para el acceso interno, mediante una URL privada.

Se trata de una función y un tema avanzados. Si no conoce las puertas de enlace de StoreFront con GSLB (Global Server Load Balancing), consulte los enlaces de información relacionada que hay al final de este artículo.

Esta función ofrece las ventajas siguientes:

- Compatibilidad con dos URL simultáneas para un mismo objeto de puerta de enlace.
- Los usuarios pueden alternar entre dos direcciones URL diferentes para acceder a Citrix 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 quiere usar.
- Períodos 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 Citrix Gateway en StoreFront dentro de la zona DMZ tanto para el acceso interno como para el externo.
- Compatibilidad con 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 Configurar almacenes multisitio con alta disponibilidad.

Consideraciones sobre la implementación cuando se usan dos direcciones URL de puerta de enlace

- El nombre de dominio completo de gatewayURL se muestra para cada puerta de enlace en la consola de administración de StoreFront. La propiedad GSLBURL de cada puerta de enlace solo es visible mediante el uso de cmdlets de PowerShell.
- Las aplicaciones nativas de Citrix Receiver y Citrix Workspace utilizan gatewayURL para la autenticación.
- gatewayURL se incluye en la etiqueta de ubicación del archivo de aprovisionamiento (receiver.cr) utilizado para configurar las aplicaciones de Citrix Receiver y Citrix Workspace con información de almacenes y puertas de enlace.
- Utilice el PowerShell proporcionado para modificar los archivos web.config de almacén e itinerancia. No lo haga manualmente.

> **Importante:**
>
> Antes de configurar una segunda dirección URL de puerta de enlace mediante el parámetro -gslburl, revise 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 Citrix Gateway y StoreFront deben estar presentes en los certificados del servidor. Para obtener más información acerca de certificados de servidor, consulte Planificar el uso de la puerta de enlace y el servidor de certificados.

DNS

- **DNS dividido**. 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 que admita esto.
- **Una misma URL para el acceso interno y externo a los recursos publicados**. Debe decidir si quiere utilizar la misma dirección URL para acceder a recursos publicados desde fuera y desde dentro de la red corporativa. Si no, considere si la posibilidad de tener direcciones URL distintas sería aceptable. Por ejemplo: `example.com` y `example.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 de StoreFront.

```
1 loadbalancer.storefront.example.net
2 server1.storefront.example.net
3 server2.storefront.example.net
4 server3.storefront.example.net
```

Establezca la URL base del host del grupo de servidores de StoreFront para que sea el nombre de dominio completo compartido, que recurre a la dirección IP del equilibrador de carga:


```
loadbalancer.storefront.example.net
```

Ejemplo de certificado de servidor para un dispositivo Citrix Gateway al que se accede de forma externa e interna mediante un 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

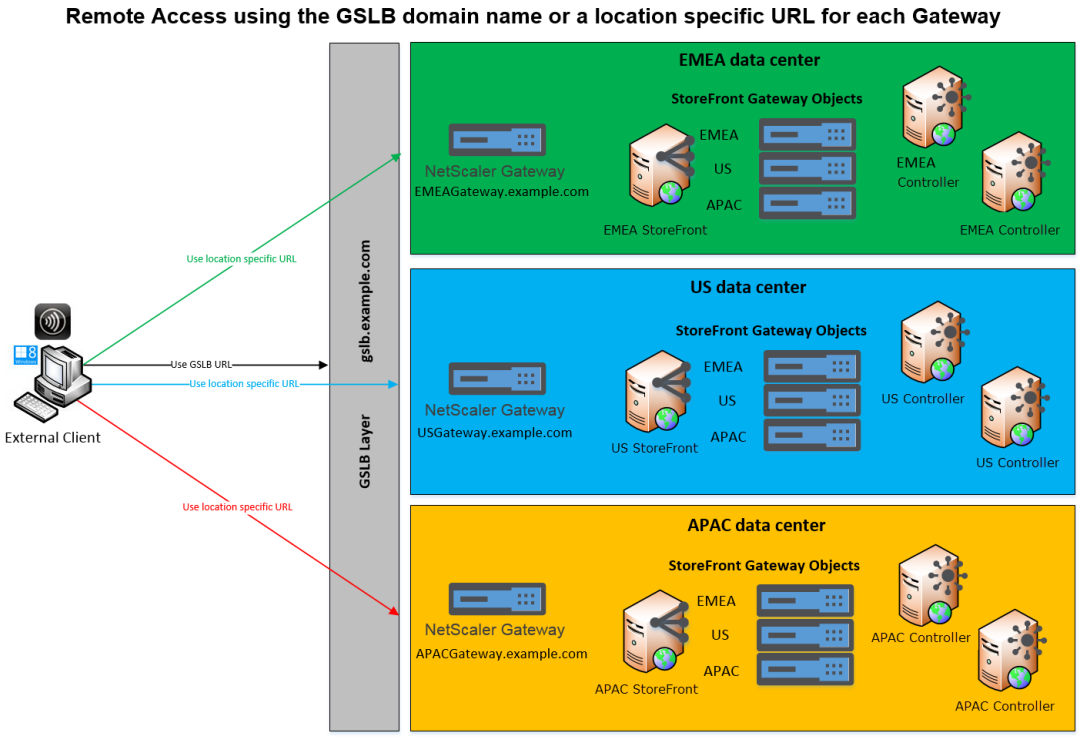
Un certificado de servidor SAN firmado públicamente para el acceso externo a través de GSLB debe contener los nombres FQDN.

```
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 quiera mediante su nombre FQDN exclusivo.

Caso de uso n.º 1: Receiver para Web: GSLB y varios dispositivos Citrix Gateway

El administrador usa el equilibrio de carga de servidores global (GSLB) y varios dispositivos Citrix Gateway para equilibrar las conexiones remotas con recursos publicados en dos o más ubicaciones, dentro de una implementación global de Citrix de gran tamaño.



En este ejemplo:

- Cada ubicación o centro de datos contiene al menos una puerta de enlace, uno o varios servidores de StoreFront y uno o varios Controllers de XenApp y XenDesktop para ofrecer recursos publicados en esa ubicación. Cada servicio GSLB configurado en los dispositivos Citrix ADC GSLB dentro de la implementación global representa un servidor virtual VPN de puerta de enlace. Todos los servidores de StoreFront de la implementación deben estar configurados para que contengan todos los servidores virtuales de Citrix Gateway que componen la capa de GSLB. Los dispositivos Citrix 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 de StoreFront o los Controllers de Citrix Virtual Apps and Desktops 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 con la URL específica de su ubicación, hasta que se resuelvan los problemas de

GSLB.

Caso de uso n.º 1: Receiver para Web y aplicaciones de Citrix Receiver y Citrix Workspace: GSLB y varios dispositivos Citrix Gateway

Atributos de puerta de enlace

Para utilizar GSLB con aplicaciones nativas de Citrix Receiver o Citrix Workspace, utilice **Add-STFRoamingGateway** (crear) o **Set-STFRoamingGateway** (modificar) para especificar los siguientes atributos:

-GatewayUrl: Establecido como el nombre de dominio completo compartido para todas las puertas de enlace GSLB.

-GSLBurl: Establecido como el nombre FQDN único de puerta de enlace para cada puerta de enlace.

> Nota:
>
> Puede parecer poco intuitivo, pero no afecta de ninguna manera a este caso de uso web. Garantiza que las aplicaciones nativas de Citrix Receivers o Citrix Workspace reciban el nombre de dominio completo compartido que utiliza GSLB dentro del documento de detección encontrado al acceder al dispositivo de punto final `https://storefront.domain.com/citrix/<storename>/discovery`. También garantiza que el archivo de aprovisionamiento (receiver.cr) exportado por el comando **Exportar archivo de aprovisionamiento** de StoreFront contenga el nombre de dominio completo GSLB compartido.

Ejemplo de archivos de aprovisionamiento

Ejemplo de archivo 1 con `–GatewayUrl https://gslb.domain.com`. Permite que las aplicaciones nativas de Citrix Receiver o Citrix Workspace utilicen GSLB para conectarse a puertas de enlace.


```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

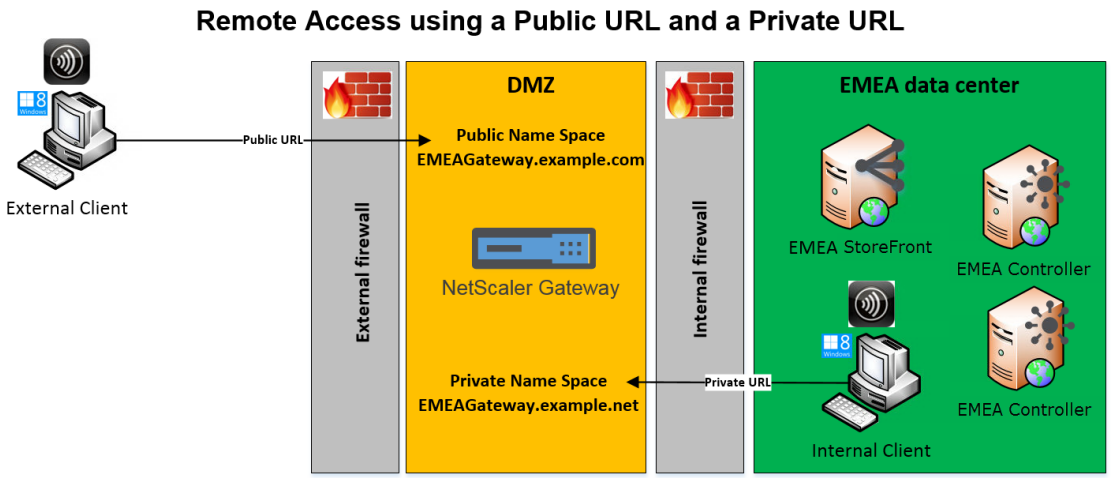
Ejemplo de archivo 2 con `-GatewayUrl https://emeagateway.domain.com, https://usgateway.domain.com and https://apacgateway.domain.com`. Permite que las aplicaciones nativas de Citrix Receiver o Citrix Workspace utilicen las URL únicas para conectarse a puertas de enlace.

```
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://emeagateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://ftlgateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://bglgateway.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

Las aplicaciones nativas de Citrix Receiver y Citrix Workspace utilizan el nombre de dominio completo compartido para la autenticación.

Caso de uso n.º 2: Un único dispositivo Citrix Gateway con una URL pública o privada

El administrador usa el mismo Citrix 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 dispositivo Citrix Gateway, incluso aunque el cliente sea interno.
- Dicho dispositivo se encuentra en una zona DMZ.
- Existen dos rutas de red distintas al dispositivo Citrix 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:

```
1 Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com" -
    SubnetIPAddress "10.0.0.1" -CallbackUrl "https://emeagateway.example
    .com" -LogonType "DomainAndRSA" -SmartCardFallbackLogonType "None" -
    Version "Version10_0_69_4" -SecureTicketAuthorityUrls "https://emea-
    controller.example.com/scripts/ctxsta.dll,https://us-controller.
    example.com/scripts/ctxsta.dll,https://apac-controller.example.com/
    scripts/ctxsta.dll"
2 Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com"
```



```
3 Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA
    gateway object)
4 Or
5 Get-STFRoamingGateway (returns all gateway object configured in
    StoreFront)
```

En caso de uso n.º 1, puede quitar GSLBurl de "EMEAGateway" al establecer su **GslbLocation** en null. El siguiente comando de PowerShell modifica el objeto de la puerta de enlace $EMEAGateway almacenada en la memoria. **Set-STFRoamingGateway** puede recibir $EMEAGateway para actualizar la configuración de StoreFront y quitar GSLBurl.

```
1 $EMEAGateway = Get-STFRoamingGateway
2 $EMEAGateway.GslbLocation = $Null
3 Set-STFRoamingGateway -Gateway $EMEAGateway
```

En el caso n.º 1, se devuelven las puertas de enlace siguientes al usar el comando **Get-STFRoamingGateway**:

```
1 Name: EMEAGateway
2 Location: https://emeagateway.example.com/ (Unique URL for the EMEA
    Gateway)
3 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)
4
5 Name: USGateway
6 Location: https://USgateway.example.com/ (Unique URL for the US Gateway
    )
7 GslbLocation: https://gslb.example.com/ (GSLB URL for all three
    gateways)
8
9 Name: APACGateway
10 Location: https://APACgateway.example.com/ (Unique URL for the APAC
    Gateway)
11 GslbLocation:  https://gslb.example.com/ (GSLB URL for all three
    gateways)
```

En el caso n.º 2, se devuelven las puertas de enlace siguientes al usar el comando **Get-STFRoamingGateway**:

```
1 Name: EMEAGateway
2 Location: https://emeagateway.example.com/ (Public URL for the Gateway)
3 GslbLocation: https://emeagateway.example.net/ (Private URL for the
    Gateway)
```

En el caso n.º 1, se devuelve el enrutamiento óptimo de puerta de enlace al usar el comando **Get-STFStoreRegisteredOptimalLaunchGateway**:


```
$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 de cada puerta de enlace se almacena 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 de StoreFront.

Caso de uso n.º 1: Puertas de enlace en el archivo web.config del servicio Roaming Service

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.1" rwmode
    ="NONE" deployment="Appliance" callbackurl=https://emeagateway.
    example.com/CitrixAuthService/AuthService.asmx sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" /><gslbLocation path=
    "https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
```



```
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<gateway id="b8ec720c-d85e-1889-8188-1cf08a2cf762" name="USGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.2" rwmode="NONE" deployment="Appliance" callbackurl="https://usgateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://usgateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>

<gateway id="c57117b5-e111-1eed-9117-a1ffa1c8100e" name="APACGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.3" rwmode="NONE" deployment="Appliance" callbackurl="https://apacgateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://apacGateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
```

```
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>
```

Caso de uso n.º 2: Puertas de enlace en el archivo web.config del servicio Roaming

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="Domain" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE" deployment="Appliance" callbackurl="https://emeagateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" />
<gslbLocation path=" https://emeagateway.example.net/" />
<clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.net/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>
```

Información relacionada

En la documentación para desarrolladores, consulte Módulos de PowerShell del SDK de Citrix StoreFront.

Configurar Citrix ADC y StoreFront para la autenticación con formularios delegada (DFA)

December 23, 2019

La autenticación extensible proporciona un único punto de personalización para la extensión de la autenticación con formularios del dispositivo Citrix ADC y StoreFront. Para lograr una solución de autenticación mediante el SDK de autenticación extensible, debe configurar la autenticación con formularios delegada (DFA) entre el dispositivo Citrix ADC 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, Citrix Gateway delega su autenticación a StoreFront, el cual interactúa con un servidor o servicio externo de autenticación.

La configuración de la autenticación con formularios delegada en Citrix Gateway se describe en CTX200383.

Recomendaciones para la instalación

- Para garantizar que la comunicación entre el dispositivo Citrix ADC 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 el dispositivo Citrix ADC 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 modules
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
    DeliveryServices.ConfigurationProvider.dll'
Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
    DeliveryServices.ConfigurationProvider.dll'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-
    DSDFAServer
Id                              : bf694fbc-ae0a-4d56-8749-
    c945559e897a
ClassType                       : e1eb3668-9c1c-4ad8-bbae-
    c08b2682c1bc
FrameworkController             : Citrix.DeliveryServices.Framework
    .FileBased.FrameworkController
ParentInstance                  : 8dd182c7-f970-466c-ad4c-27
    a5980f716c
RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375
    d79634b3
TenantId                        : 860e9401-39c8-4f2c-928d-34251102
    b840
Data                            : {
  }

ReadOnlyData                    : {
 [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin
    , Citrix.DeliverySer
                                  vices.Web.Commands], [Tenant, 860
                                      e9401-39c8-4f2c-928d-34251102
                                      b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [
    ParentInstanceId, 8dd182c7-f
                                  970-466c-ad4c-27a5980f716c], [
                                      TenantId, 860e9401-39c8-4f2c
```



```
                                        -928d-34251102b840] }
25
26 AdditionalInstanceDependencies : {
27  b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }
28
29 IsDeployed                      : True
30 FeatureClass                    : Citrix.DeliveryServices.Framework
       .Feature.FeatureClass
```

2. Agregue el Citrix Trusted Client. Configure la clave secreta compartida (frase de contraseña) entre StoreFront y el dispositivo Citrix ADC. La frase de contraseña y el ID del cliente deben ser idénticos a los que configuró en el dispositivo Citrix ADC.

```
1 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. Esto es un ejemplo de lo que puede ver.

```
1  <example connectorURL="http://Example.connector.url:8080/adapters-
       sf-aaconnector-webapp">
2     <routeTable order="1000">
3       <routes>
4         <route name="StartExampleAuthentication" url="Example-
              Bridge-Forms/Start">
5           <defaults>
6             <add param="controller" value="
                  ExplicitFormsAuthentication" />
7             <add param="action" value="AuthenticateStart" />
8             <add param="postbackAction" value="Authenticate" />
9             <add param="cancelAction" value="CancelAuthenticate"
                   />
10            <add param="conversationFactory" value="
                  ExampleBridgeAuthentication" />
11            <add param="changePasswordAction" value="
                  StartChangePassword" />
12            <add param="changePasswordController" value="
                  ChangePassword" />
13            <add param="protocol" value="CustomForms" />
14          </defaults>
15        </route>
```


4. En PowerShell, establezca la Conversation Factory de la autenticación con formularios delegada. En este ejemplo, se establece como 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**.

Desinstale StoreFront

Antes de desinstalar StoreFront, desinstale todos los plug-ins externos de autenticación, ya que afectará a la funcionalidad de StoreFront.

Autenticarse con dominios distintos

March 2, 2020

Algunas organizaciones han establecido directivas que no les 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 Citrix Gateway. Luego, puede usar otro dominio para autenticarse en StoreFront y el sitio de Receiver para Web. La autenticación a través de Citrix 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 nativos móviles o de escritorio procedentes de Citrix Receiver o de aplicaciones Citrix Workspace.

Configurar 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:

- Citrix 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`

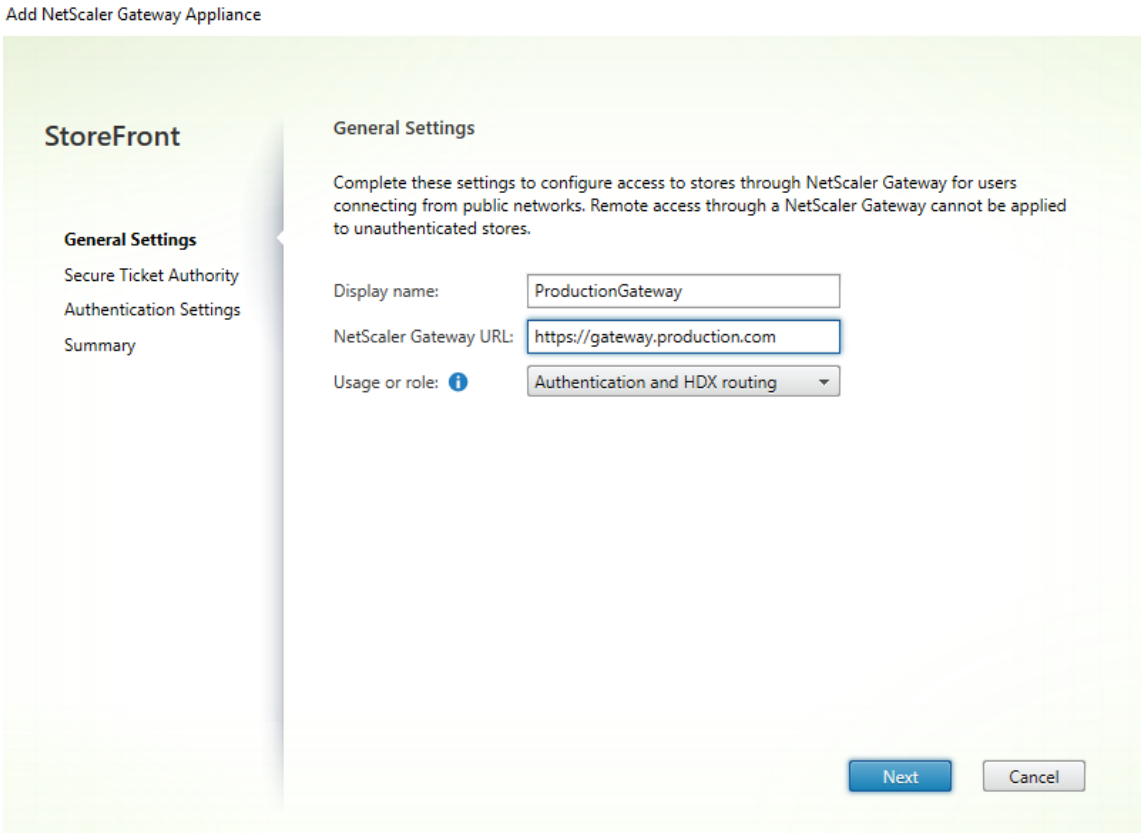
Configuración del dominio `development.com` utilizado en este ejemplo:

- StoreFront, Citrix Virtual Apps and Desktops y VDA se encuentran 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.

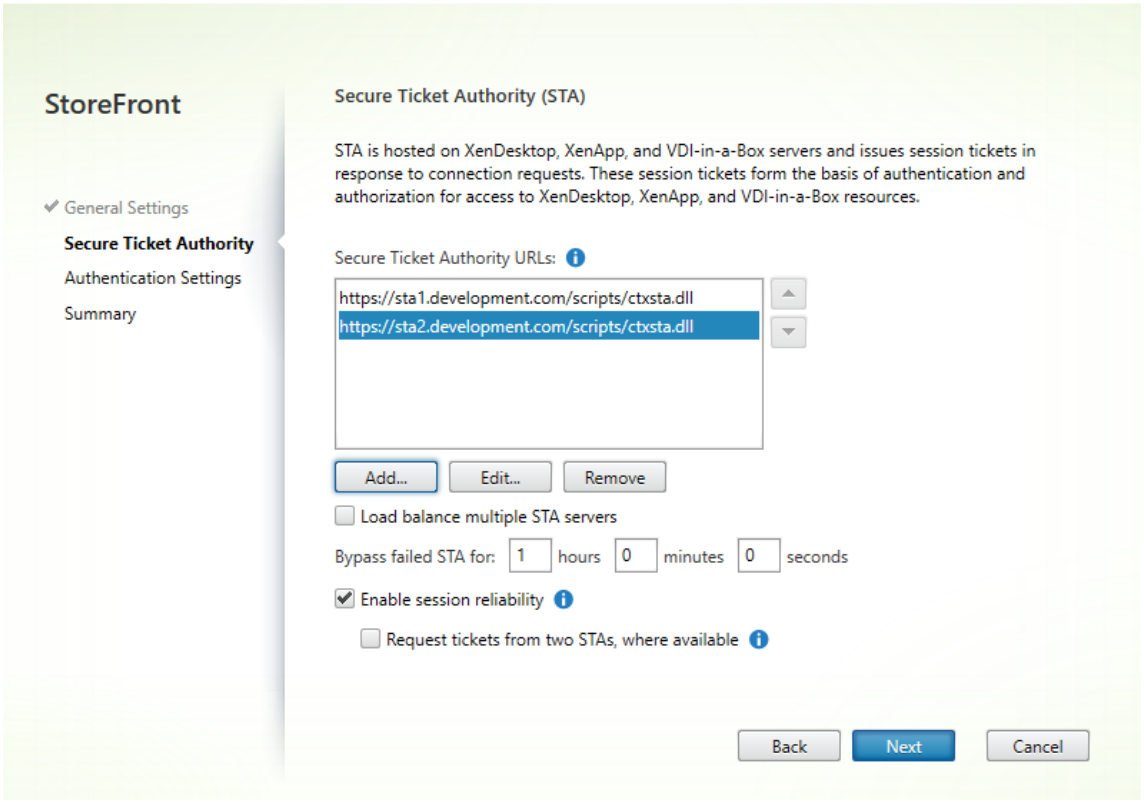
Configurar Citrix Gateway para el almacén

Para configurar Citrix Gateway para el almacén:

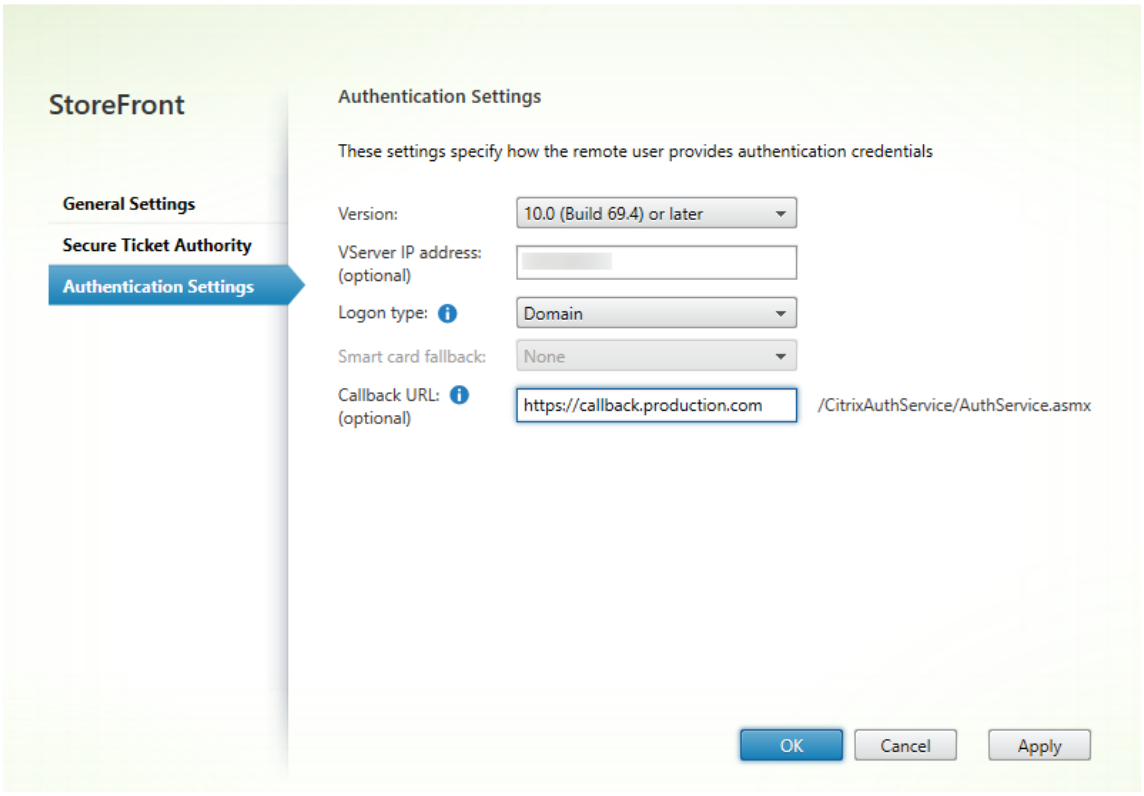
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel **Acciones**, haga clic en **Administrar Citrix Gateway**.
2. En la pantalla "Administrar Citrix Gateway", haga clic en **Agregar**.
3. Complete los pasos de Configuración general, de Secure Ticket Authority y de Autenticación.



Add NetScaler Gateway Appliance



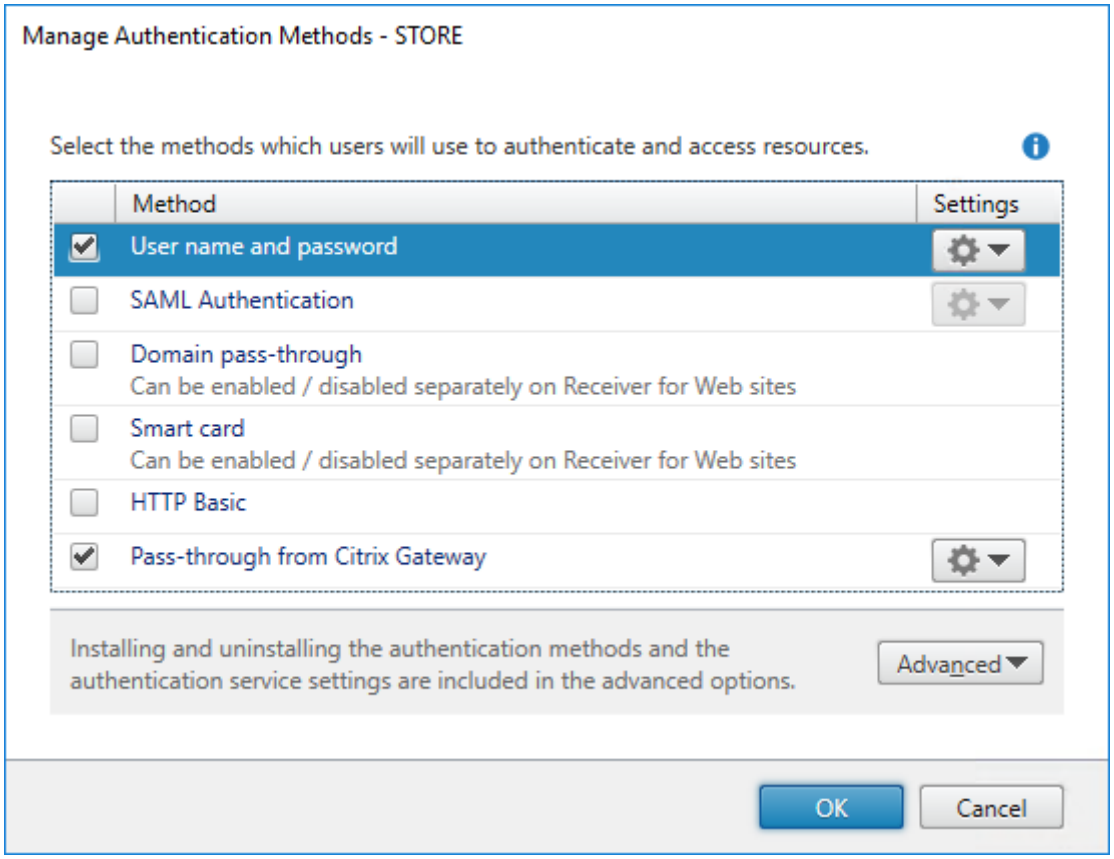
Edit NetScaler Gateway appliance - ProductionGateway



> **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. El dispositivo Citrix ADC 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`. Si no, también se puede utilizar un nombre FQDN de `development.com` que recurra a la IP virtual (VIP) del servidor virtual de Citrix Gateway.

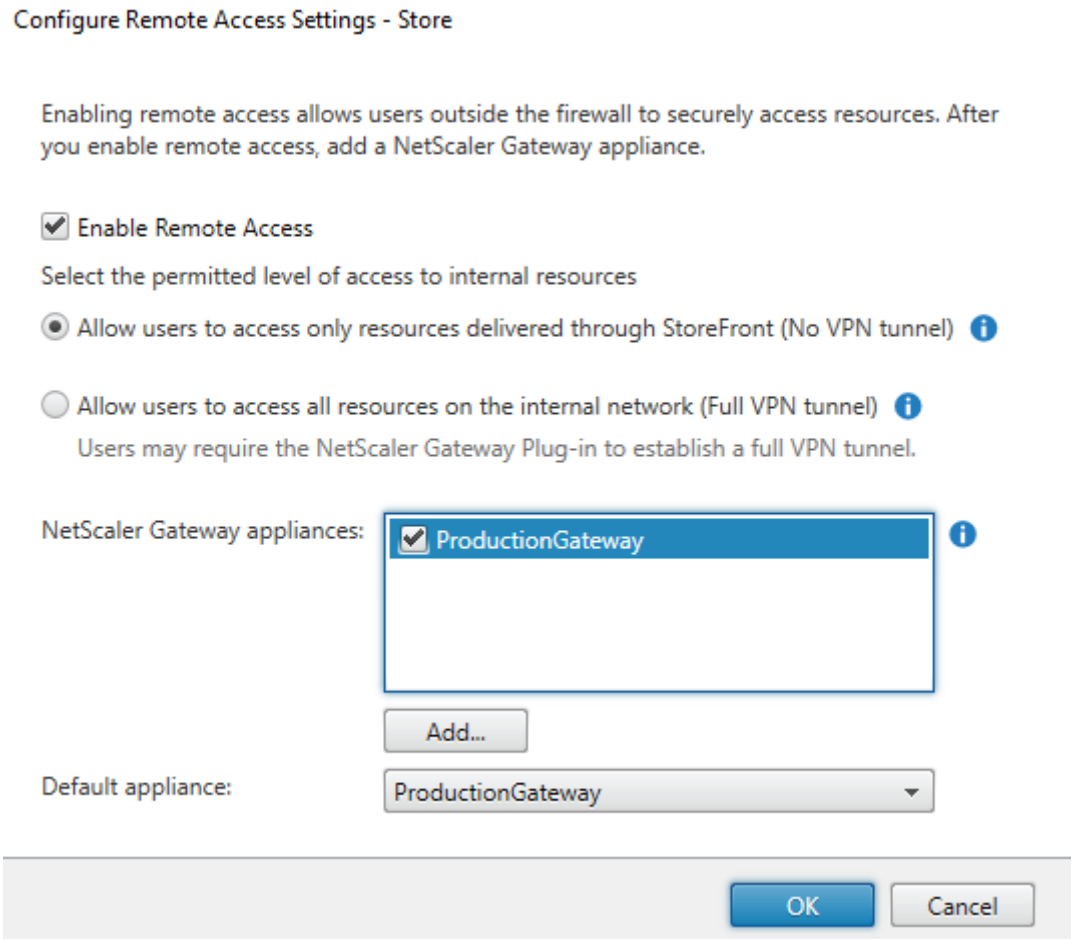
Habilitar PassThrough desde Citrix Gateway

1. Seleccione **Almacenes** 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 Citrix Gateway**.
3. Haga clic en **Aceptar**.



Configurar el almacén para el acceso remoto a través de Gateway

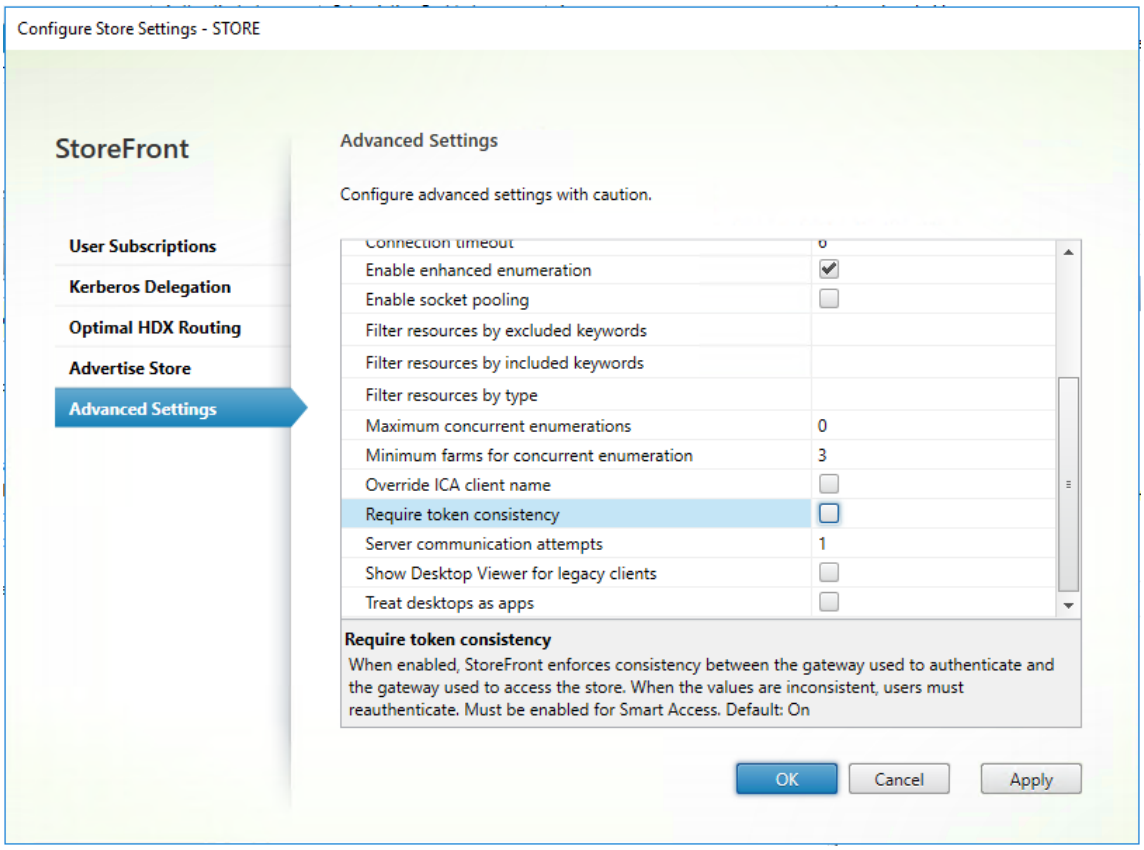
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros de acceso remoto**.
2. Seleccione **Habilitar acceso remoto**.
3. Compruebe que ha registrado el dispositivo Citrix Gateway en el almacén. Si no lo registra, la generación de tíquets STA no funcionará.



Inhabilitar la coherencia de tokens

1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront y, en el panel de resultados, seleccione un almacén. En el panel **Acciones**, haga clic en **Configurar parámetros del almacén**.
2. En la página Configurar parámetros del almacén, seleccione **Parámetros avanzados**.
3. Desmarque la casilla **Requerir coherencia de token**. Para obtener más información, consulte Parámetros avanzados de los almacenes.

4. Haga clic en **Aceptar**.



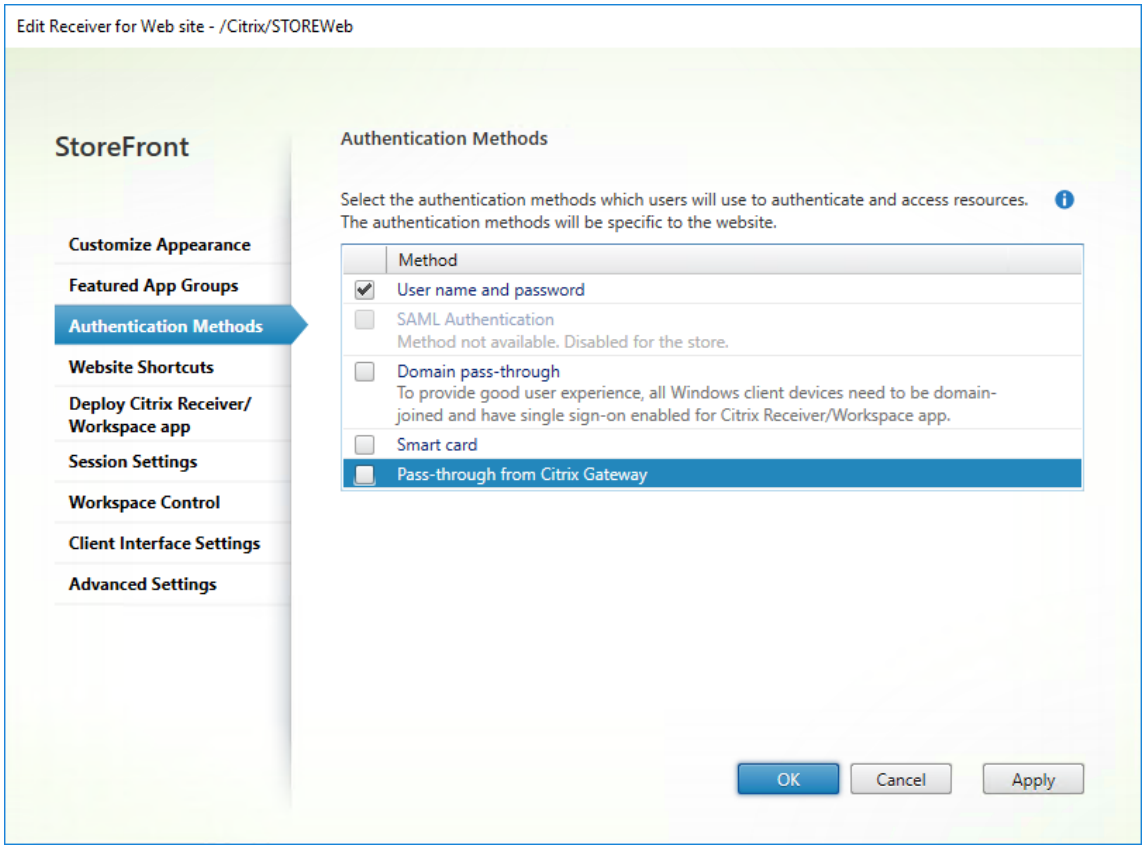
> Nota:
>
> El parámetro "Requerir coherencia de token" está marcado (activado) de forma predeterminada. Si lo inhabilita, las funciones de SmartAccess utilizadas para Citrix ADC End Point Analysis (EPA) dejan de funcionar. Para obtener más información sobre SmartAccess, consulte CTX138110.

Inhabilitar la autenticación PassThrough desde Citrix Gateway para el sitio de Receiver para Web

> **Importante:**
>
> Inhabilitar la autenticación PassThrough desde Citrix Gateway impide que Receiver para Web use las credenciales incorrectas del dominio `production.com` transferido desde el dispositivo Citrix ADC. Inhabilitar la autenticación PassThrough desde Citrix 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 Citrix Gateway.

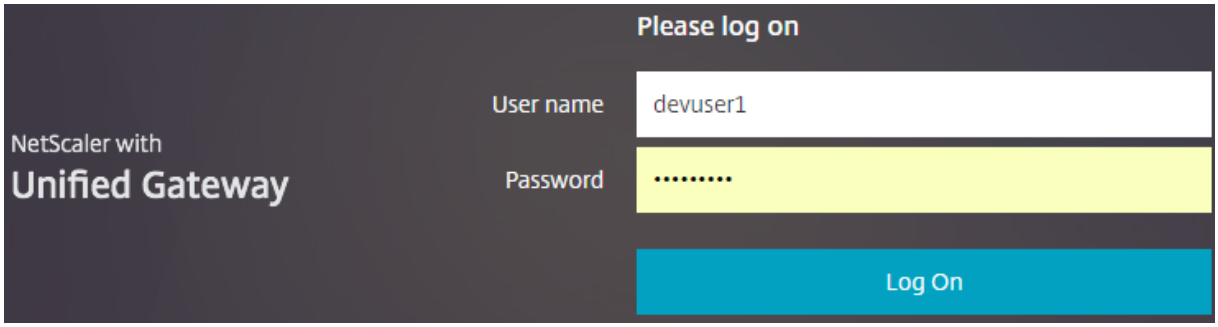
1. Seleccione el nodo **Almacenes** en el panel izquierdo de la consola de administración de Citrix StoreFront.
2. Seleccione el **almacén** que quiere modificar.

3. En el panel **Acciones**, haga clic en **Administrar sitios de Receiver para Web**.
4. En Métodos de autenticación, desmarque **PassThrough desde Citrix Gateway**.
5. Haga clic en **Aceptar**.

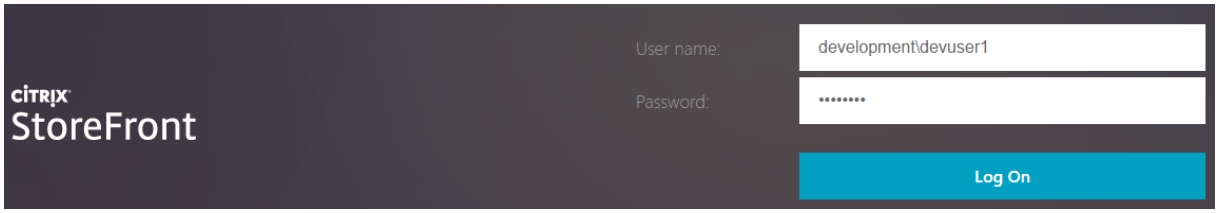


Iniciar sesión en Gateway con el usuario y las credenciales de `production.com`

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`.

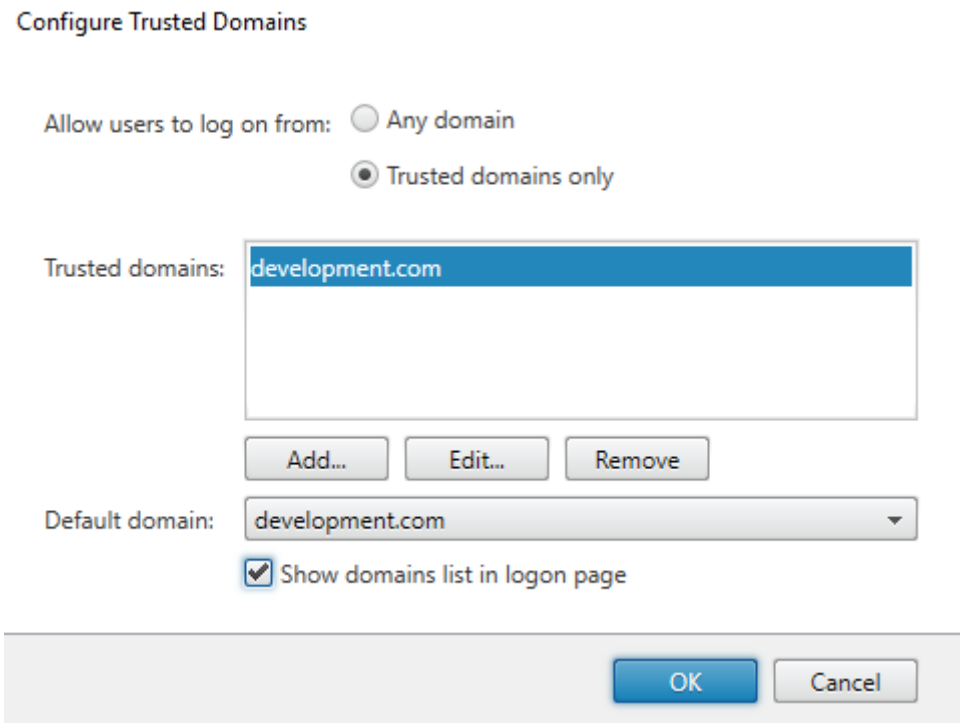


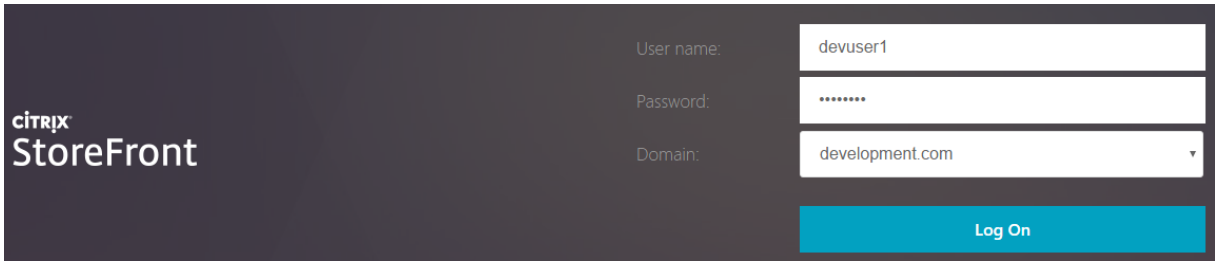
Agregar una lista desplegable de dominios de confianza en StoreFront (opcional)

Este parámetro es optativo, pero puede contribuir a evitar que el usuario introduzca accidentalmente el dominio incorrecto para autenticarse a través de Citrix 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 Citrix 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 **Almacenes** 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**.

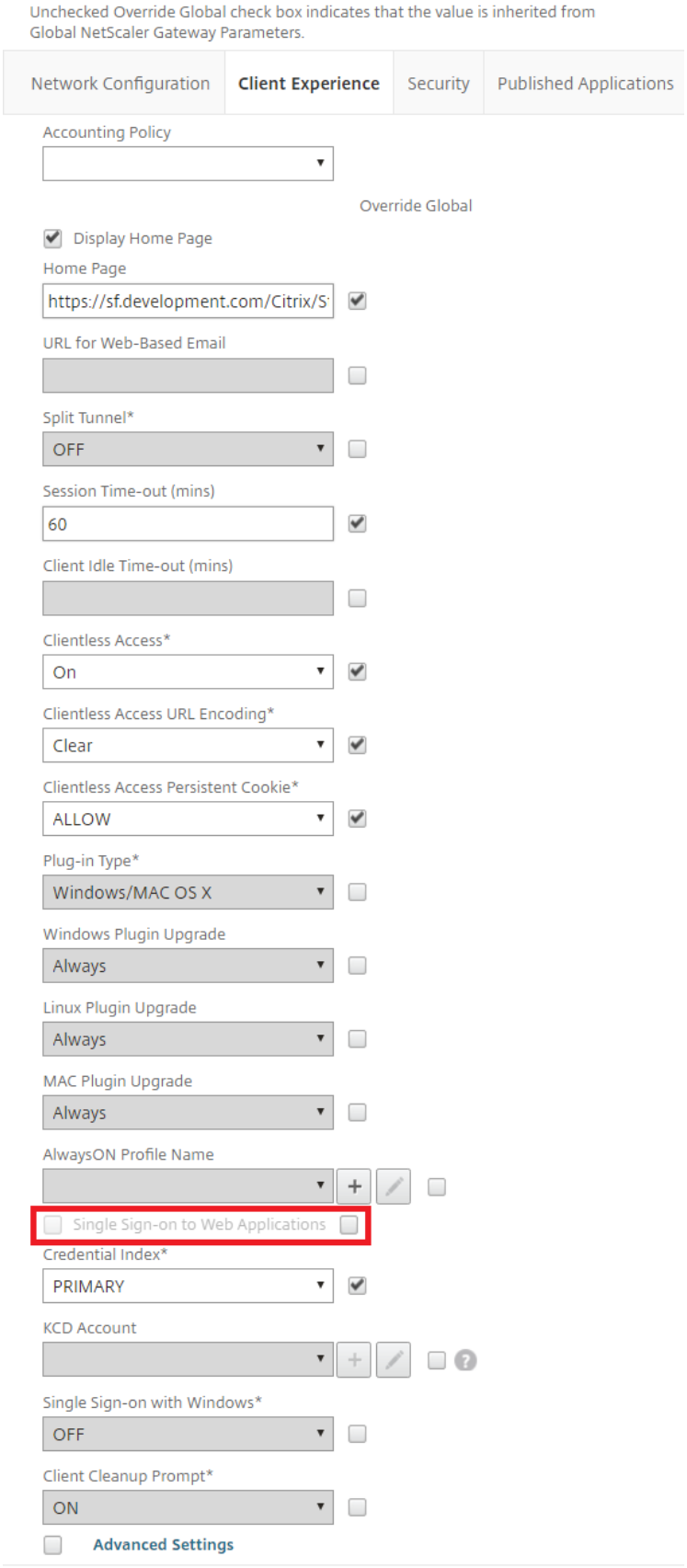


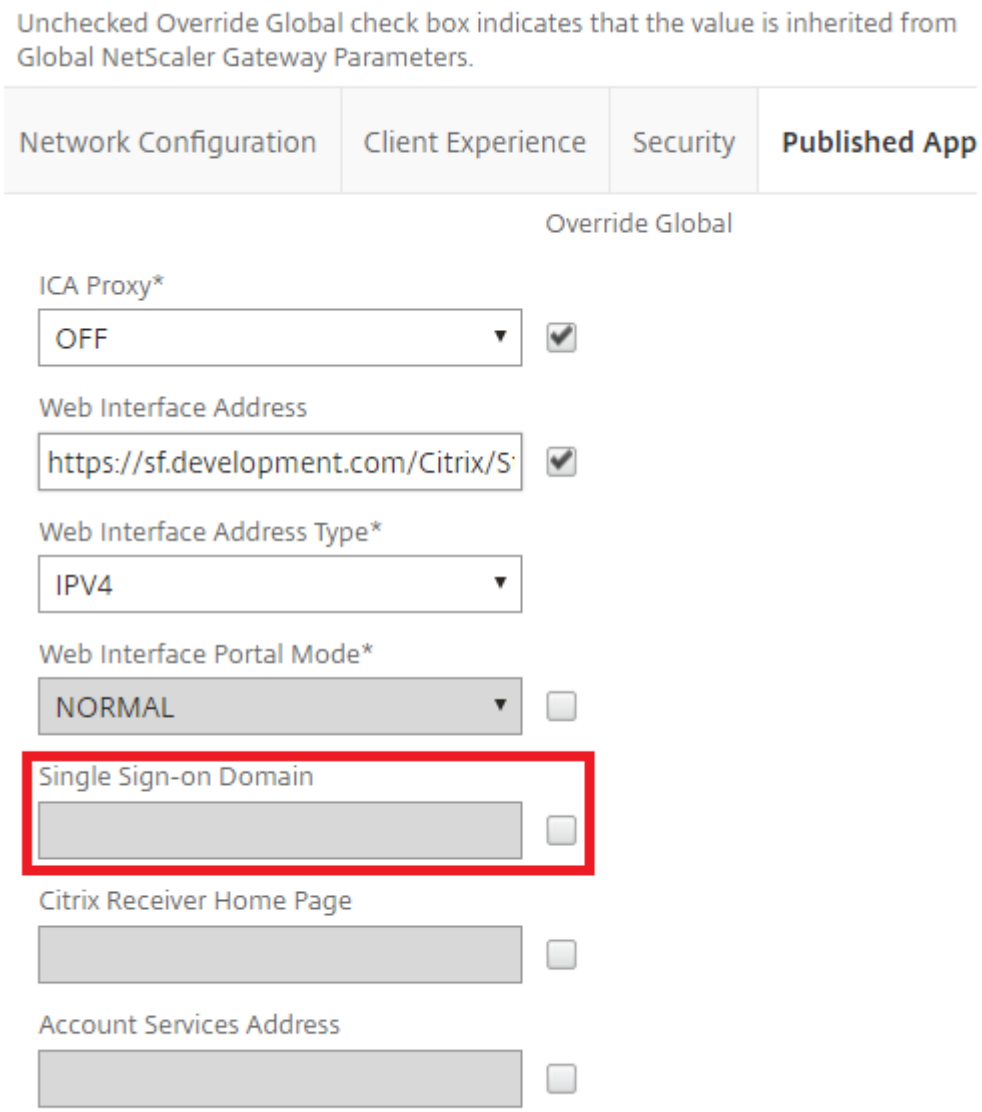


> **Nota:**
>
> En este caso de autenticación, no se recomienda que el explorador web tenga habilitado el almacenamiento en caché de las contraseñas. Si los usuarios tienen contraseñas diferentes para las dos cuentas de dominios distintos, el almacenamiento en caché de las contraseñas puede dar lugar a una mala experiencia de usuario.

Directiva de acción en la sesión de VPN (CVPN) sin cliente de Citrix Gateway

- Si se habilita el inicio Single Sign-On a las aplicaciones web en la directiva de sesiones de Citrix Gateway, las credenciales incorrectas que envíe el dispositivo Citrix ADC a Receiver para Web se ignoran porque se ha inhabilitado el método de autenticación **PassThrough desde Citrix 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 el dispositivo Citrix ADC no modifica el comportamiento que se describe en este artículo.





Configurar balizas

August 22, 2019

Utilice la tarea “Administrar balizas” para especificar las direcciones URL para utilizarlas como balizas. Estas URL pueden pertenecer tanto a la red interna como a la externa. La aplicación Citrix Workspace 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 a una aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan de-

volver los correspondientes datos de conexión a la aplicación Citrix Workspace. Esto garantiza que no se pida a los usuarios que vuelvan a iniciar sesión al acceder a un escritorio o a una aplicación.

Por ejemplo: si la baliza interna es accesible, esto indica que el usuario está conectado a la red local. Sin embargo, si la aplicación Citrix Workspace 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 lo tanto, el usuario tendrá que conectarse a escritorios y aplicaciones a través de Citrix 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 Citrix Gateway a través del que debe redirigirse 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 Citrix Gateway que usted agrega se utilizan como balizas externas de forma predeterminada.

Si cambia una baliza, asegúrese de que los usuarios actualicen la aplicación Citrix Workspace con la información actualizada. Cuando se configura un sitio de Receiver para Web para un almacén, los usuarios pueden obtener un archivo de aprovisionamiento actualizado de la aplicación Citrix Workspace del sitio. De lo contrario, puede exportar un archivo de aprovisionamiento para el almacén y hacer que este archivo esté disponible para sus usuarios.

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

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 **Almacenes** 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 URL que se utilizará 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 (`http://example.com`), no el nombre abreviado NetBIOS (`http://example`). Esto permite que la aplicación Citrix Workspace 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.

Crear un nombre de dominio completo (FQDN) para acceder a un almacén de forma interna y externa

January 31, 2020

Puede proporcionar acceso a los recursos desde la red corporativa o desde Internet a través de Citrix Gateway y simplificar la experiencia de los usuarios mediante la creación de un único nombre de dominio completo para clientes internos y clientes externos itinerantes.

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 la aplicación Citrix Workspace

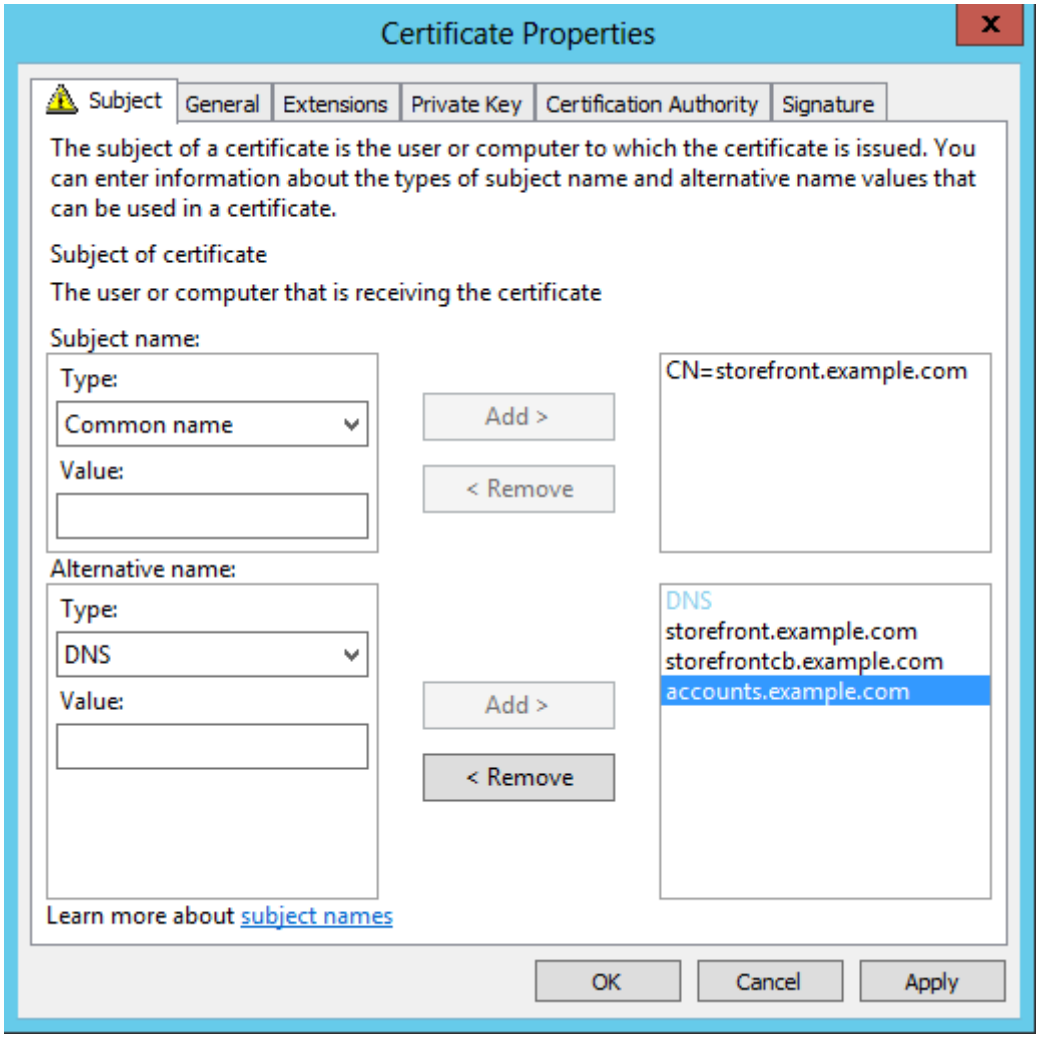
La aplicación Citrix Workspace intenta comunicarse con las balizas y usa las respuestas para determinar si los usuarios están conectados a redes locales o públicas. Cuando un usuario accede a un escritorio o a una aplicación, la información de ubicación se transfiere al servidor que proporciona el recurso para que se puedan devolver los correspondientes datos de conexión a la aplicación Citrix Workspace. Esto garantiza que no se pida a los usuarios que vuelvan a iniciar sesión al acceder a un escritorio o a una aplicación. Para obtener información sobre la configuración de balizas, consulte Configurar balizas.

> Nota:
>
> En este artículo, las menciones de “aplicación Citrix Workspace” también se aplican a las versiones compatibles de Citrix Receiver, a menos que se indique lo contrario.

Configurar el certificado SSL y del servidor virtual de Citrix Gateway

El nombre de dominio completo compartido recurre a la dirección IP de la interfaz del enrutador de un firewall externo, o bien a la dirección IP del servidor virtual de Citrix 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 al almacén de forma externa. Al utilizar una entidad de certificación (CA) raíz de terceros como Verisign en lugar de una Entidad de certificación (CA) de la empresa para firmar el certificado de la puerta de enlace, cualquier cliente externo confía automáticamente en el certificado vinculado al servidor virtual de la puerta de enlace. Si utiliza una CA raíz de terceros como Verisign, no es necesario importar certificados de CA raíz adicionales a clientes externos.

Para implementar un único certificado con el nombre común del nombre de dominio completo compartido en Citrix Gateway y en el servidor de StoreFront, tenga en cuenta si quiere que dispongan de detección remota. Si es que sí, compruebe que el certificado cumple con las especificaciones de los nombres alternativos del firmante.



Certificado de ejemplo del servidor virtual de Citrix 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 o Subject Alternative Name).
2. Compruebe también que la clave privada se puede exportar para que el certificado y la clave se puedan importar en Citrix Gateway.
3. Asegúrese de que Autorización predeterminada tenga el valor Permitir.
4. Firme el certificado con una entidad de certificación de terceros, como Verisign o una CA raíz de la empresa para su organización.

Ejemplos de nombres SAN de grupos de servidores de dos nodos

`storefront.example.com` (obligatorio)

`storefrontcb.example.com` (obligatorio)

`accounts.example.com` (obligatorio)

`storefrontserver1.example.com` (optativo)

`storefrontserver2.example.com` (optativo)

Firmar el certificado SSL del servidor virtual de Citrix Gateway con una entidad de certificación (CA)

Según sus requisitos, tiene dos opciones para elegir el tipo de certificado de CA.

- Opción 1: Certificado firmado por una entidad de certificación externa. Si el certificado enlazado al servidor virtual de Citrix Gateway está firmado por una entidad externa de confianza, es muy posible que los clientes externos NO necesiten copiar certificados de CA raíz a 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 Citrix 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 utiliza dispositivos portátiles con que tengan un Receiver nativo instalado, como iPhones y iPads, cree un perfil de seguridad en estos dispositivos.

Importar el certificado raíz en dispositivos portátiles

- Los dispositivos iOS pueden importar archivos de certificado .CER x.509 mediante archivos adjuntos de correo electrónico, ya que, por lo general, no es posible acceder al almacenamiento local de los dispositivos iOS.
- Los dispositivos Android requieren el mismo formato .CER x.509. El certificado se puede importar desde el almacenamiento local del dispositivo o desde los datos adjuntos de un correo electrónico.

DNS externo: storefront.ejemplo.com

Compruebe que la resolución de DNS proporcionada por el proveedor de servicios de Internet de la organización recurre a la dirección IP del enrutador del firewall que apunta al exterior en el borde

exterior de la DMZ o en la dirección IP virtual del servidor virtual de Citrix Gateway.

DNS dividido

- Cuando el DNS dividido (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.

Importar certificados emitidos por una entidad de certificación Windows en Citrix Gateway

WinSCP es una útil herramienta externa y gratuita para trasladar archivos de una máquina con Windows a un sistema de archivos de Citrix Gateway. Copie los certificados que quiere importar en la carpeta /nsconfig/ssl/ del sistema de archivos de Citrix Gateway. Puede usar las herramientas de OpenSSL en Citrix Gateway para extraer el certificado y la clave de un archivo PKCS12 / PFX y así crear dos archivos X.509 separados (.CER y .KEY) en formato PEM que Citrix Gateway puede utilizar.

1. Copie el archivo PFX a /nsconfig/ssl, en el dispositivo Citrix Gateway o en VPX.
2. Abra la interfaz de línea de comandos de Citrix Gateway.
3. Para pasarse al shell de FreeBSD, escriba **Shell** para salir de la interfaz de línea de comandos de Citrix 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 se le pida.
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 Citrix Gateway, escriba Exit.

Directiva de sesión para Citrix Gateway, Citrix Receivers para Windows o Citrix Receivers para Mac

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

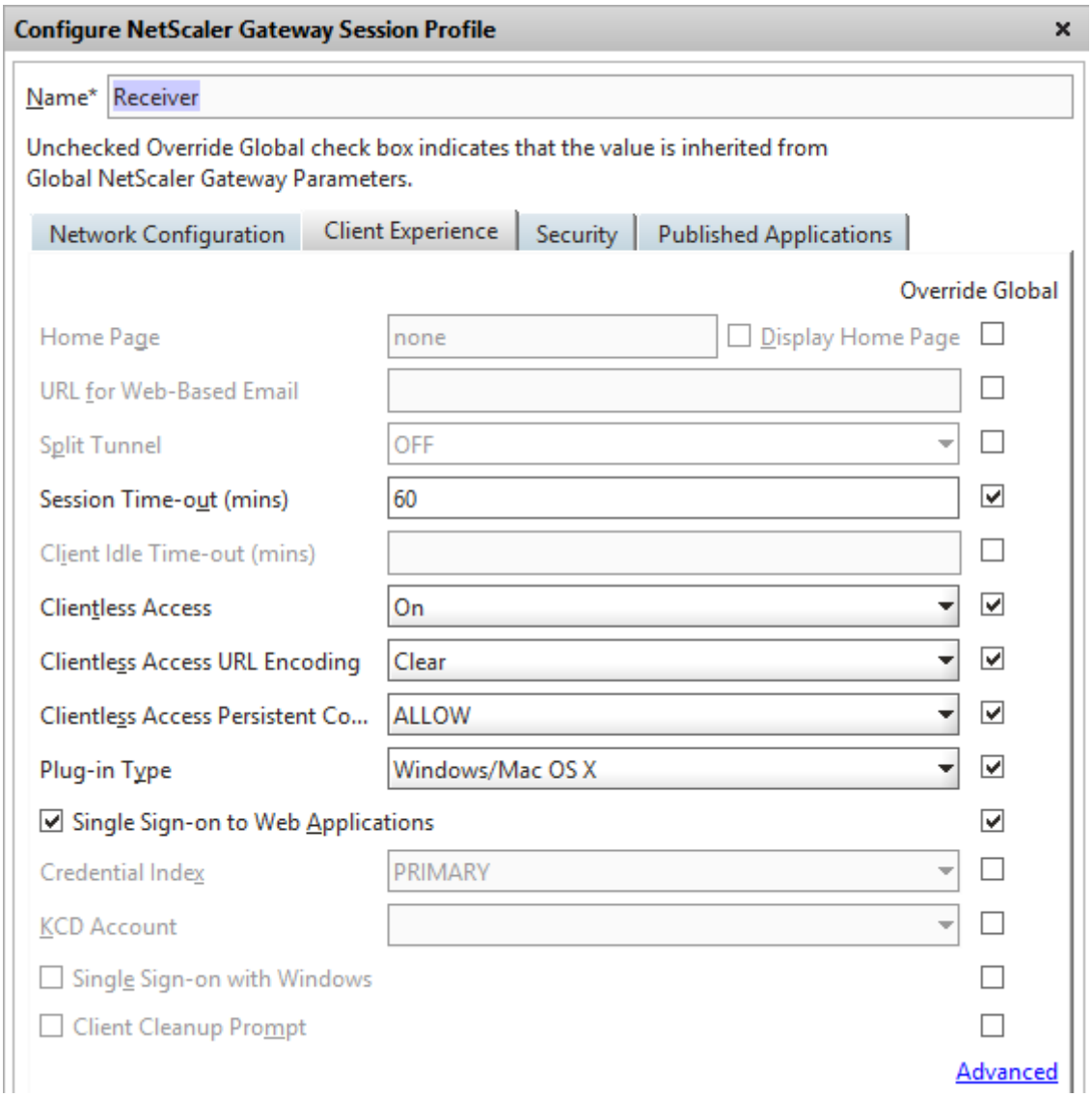
Directiva de sesiones de puerta de enlace de Receiver para Web

REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

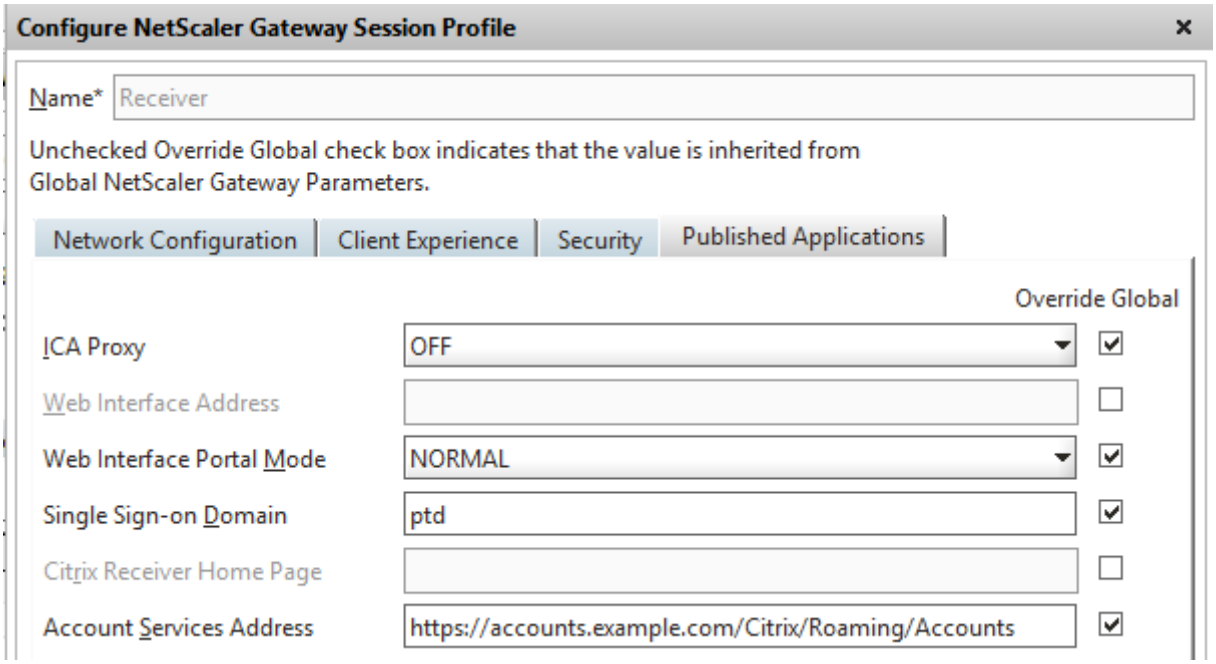
Parámetros de cVPN y SmartAccess

Si usa el modo de acceso inteligente (SmartAccess), habilítelo en la página de propiedades del servidor virtual de Citrix Gateway. Se necesitan licencias universales para cada usuario concurrente o simultáneo que accede a recursos remotos.

Perfil de Receiver

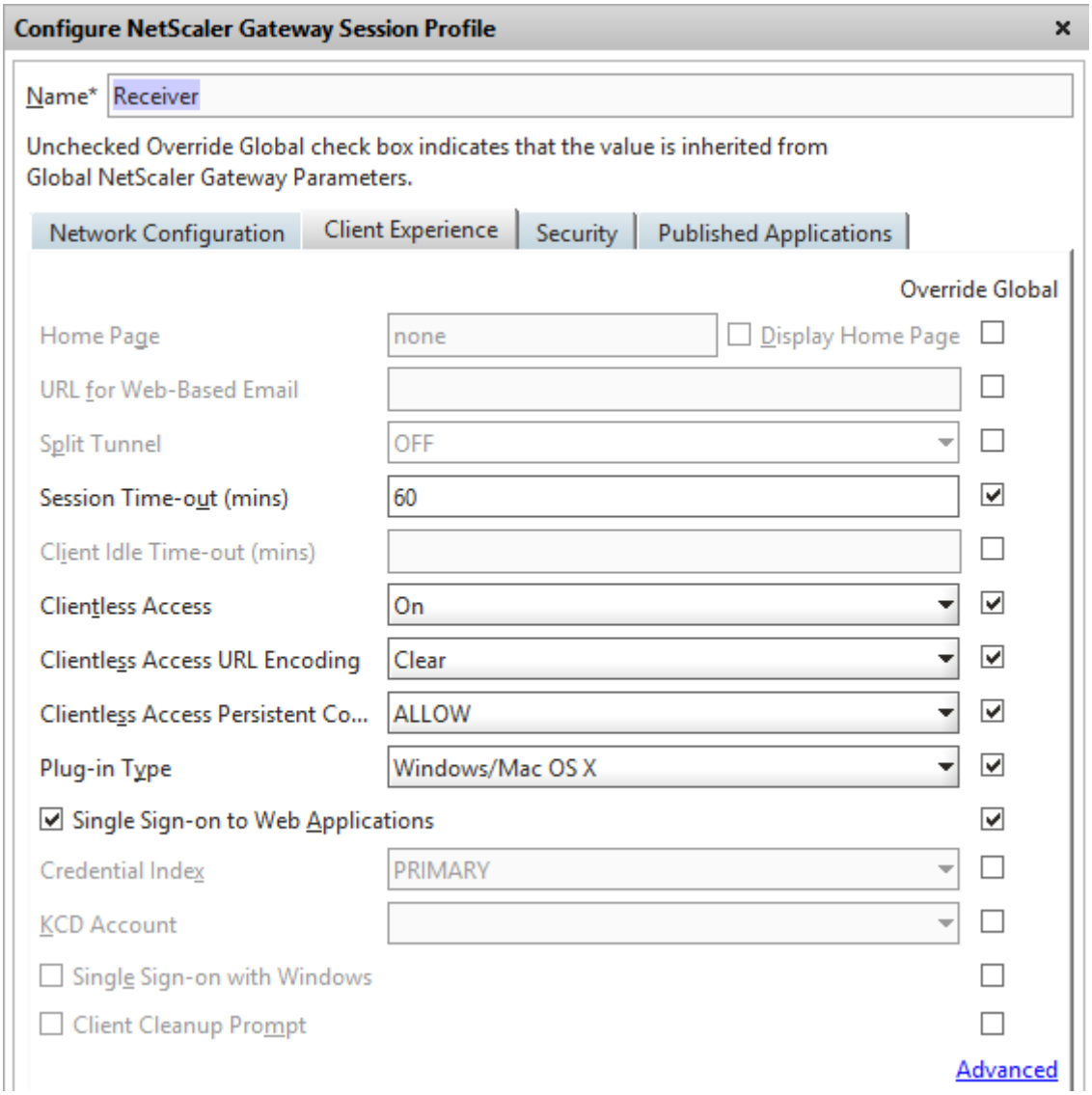


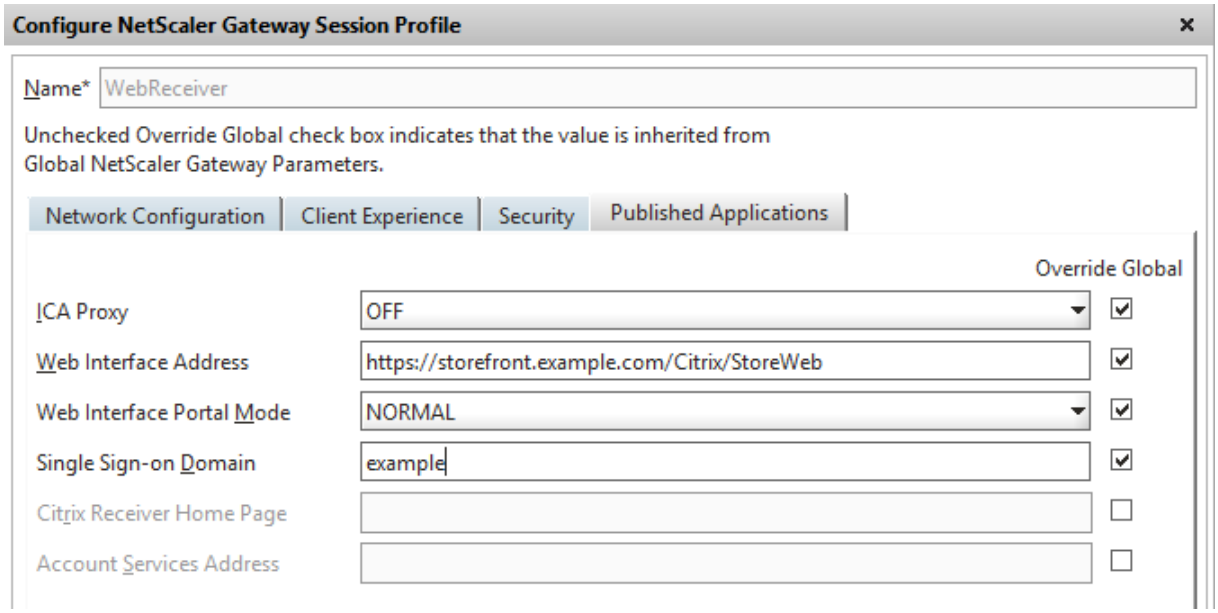
Establezca la URL del servicio de cuentas de perfil de sesión en `https://accounts.example.com/Citrix/Roaming/Accounts`NO`https://storefront.example.com/Citrix/Roaming/Accounts`.



Agregue también esta URL como una entrada de <allowedAudiences> en los archivos web.config de autenticación e itinerancia en el servidor de StoreFront. Para obtener más información, consulte “Configurar la URL base del host, la puerta de enlace y el certificado SSL de un servidor de StoreFront” en el apartado siguiente.

Perfil de Receiver para Web

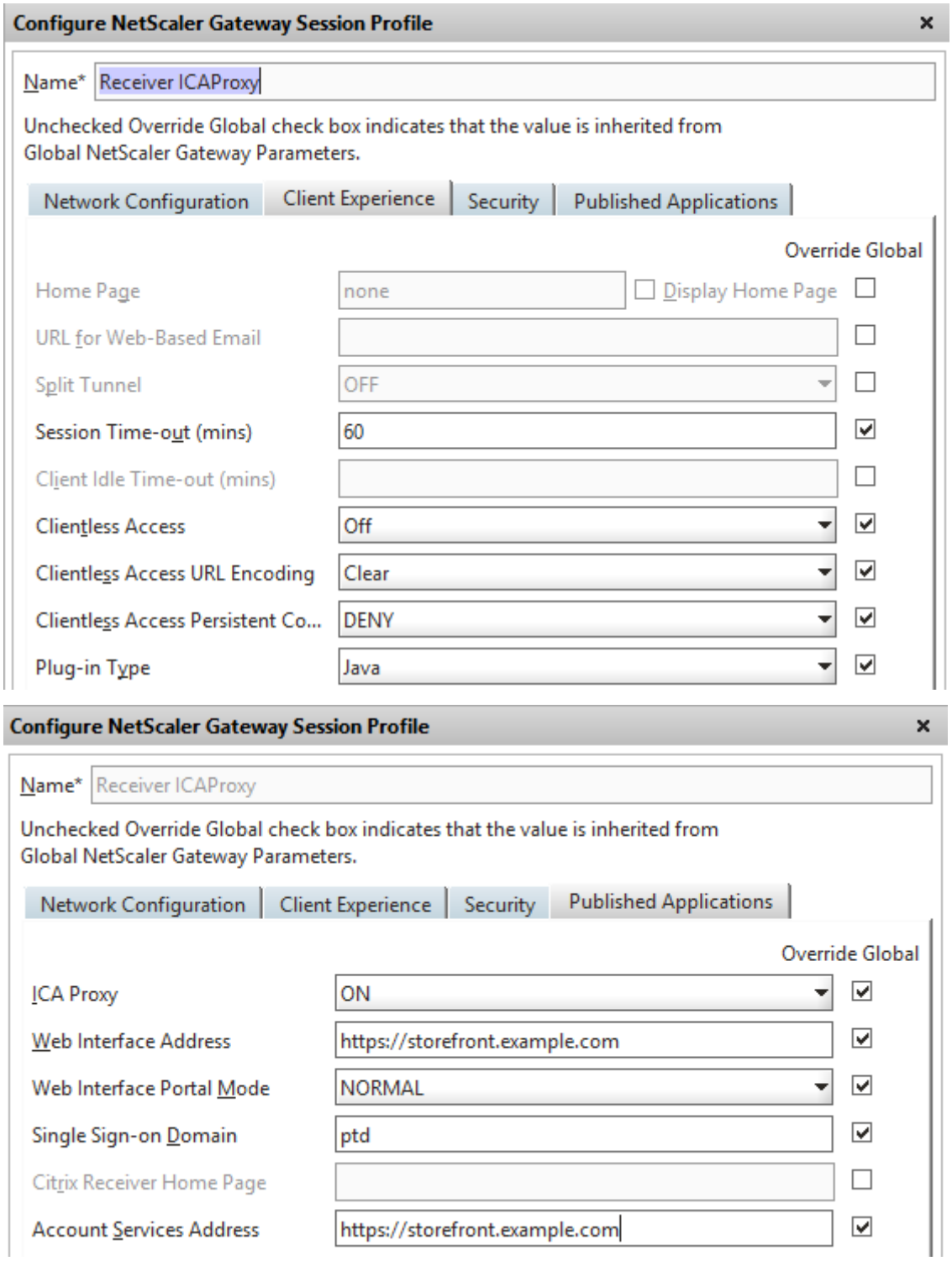




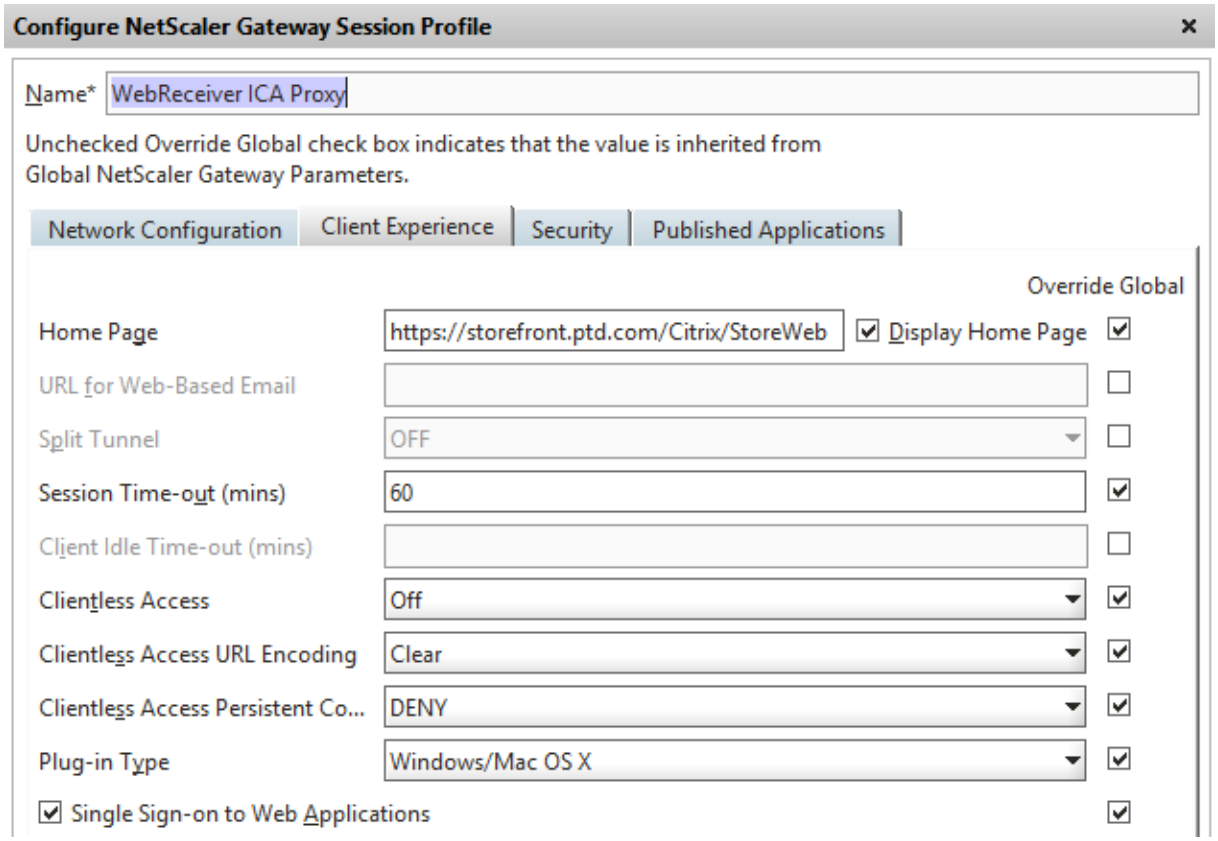
Parámetros de proxy ICA y modo Básico

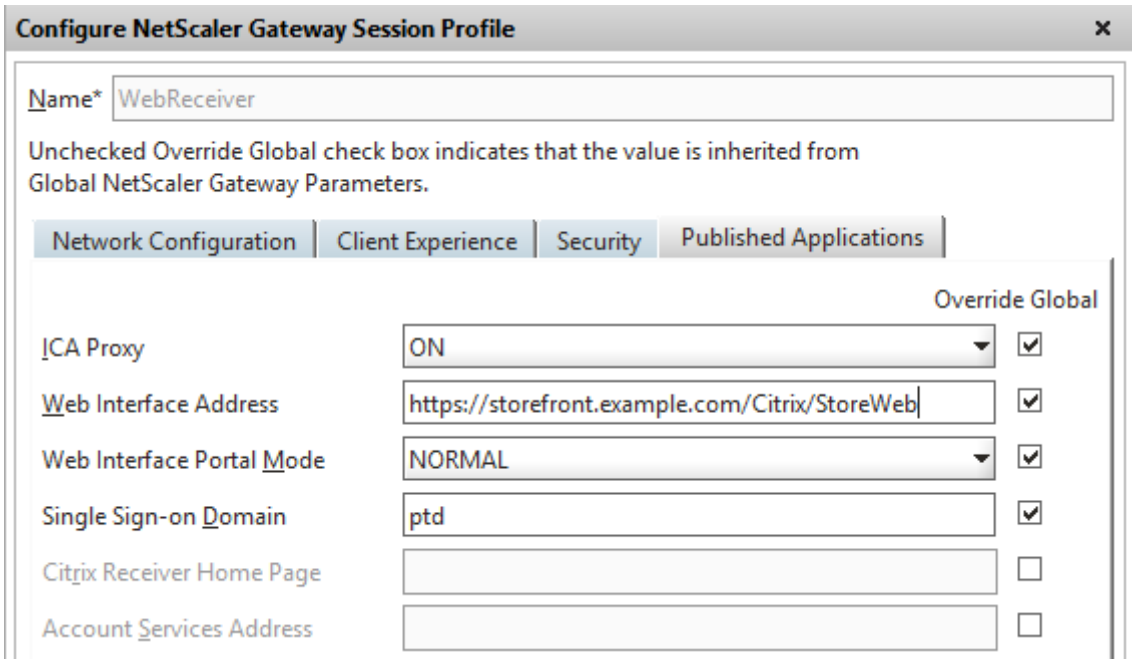
Si utiliza el proxy ICA, habilite el modo básico en la página de propiedades del servidor virtual de Citrix Gateway. Solo se necesita una licencia de plataforma de Citrix ADC.

Perfil de Receiver



Perfil de Receiver para Web





Configurar la URL base del host, la puerta de enlace y el certificado SSL de un servidor de StoreFront

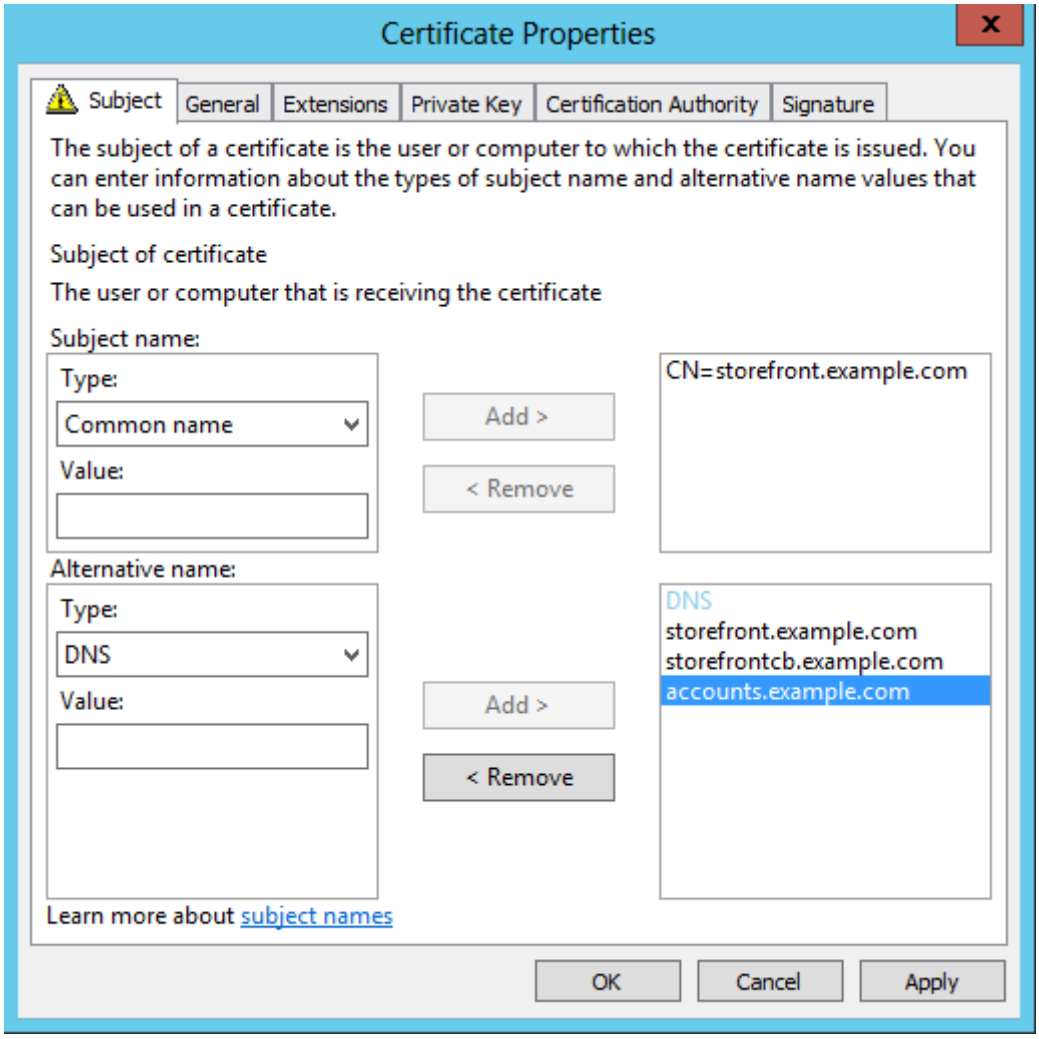
El mismo nombre de dominio completo compartido que recurre al servidor virtual de Citrix Gateway también debe recurrir directamente al equilibrador de carga de StoreFront si se ha creado un clúster de StoreFront o si hay una única dirección IP de StoreFront que aloje el almacén.

DNS interno: Cree tres registros A de DNS

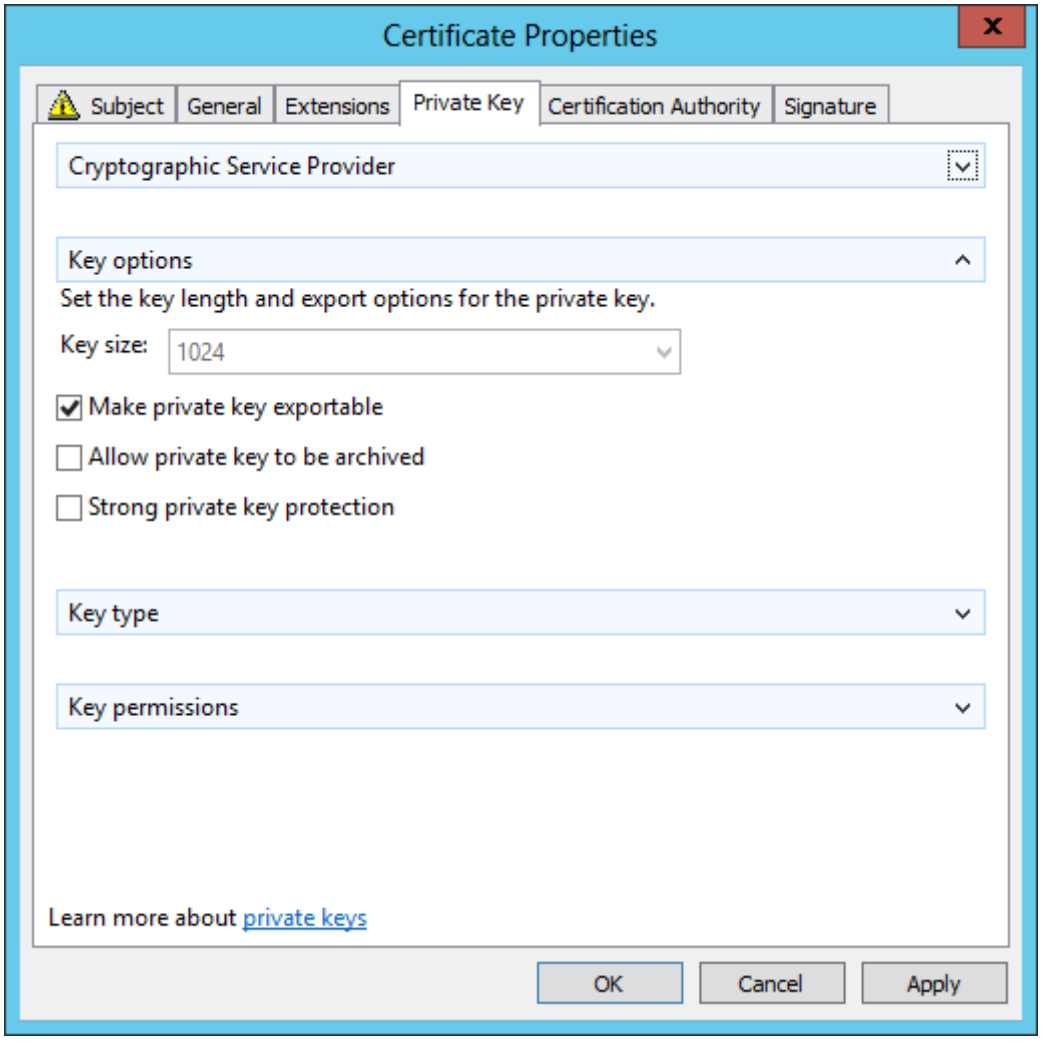
- storefront.example.com debe recurrir al equilibrador de carga de StoreFront o a la dirección IP única del servidor de StoreFront.
- storefrontcb.example.com debe recurrir a la dirección IP virtual del servidor virtual de NetScaler Gateway, de modo que, si existe un firewall entre la DMZ y la red local de la empresa, permita esto.
- accounts.example.com: Cree un alias de DNS para storefront.example.com. También recurre a la dirección IP del equilibrador de carga para el clúster de StoreFront o a la dirección IP única del servidor de StoreFront.

Certificado de ejemplo de un servidor de StoreFront: storefront.example.com

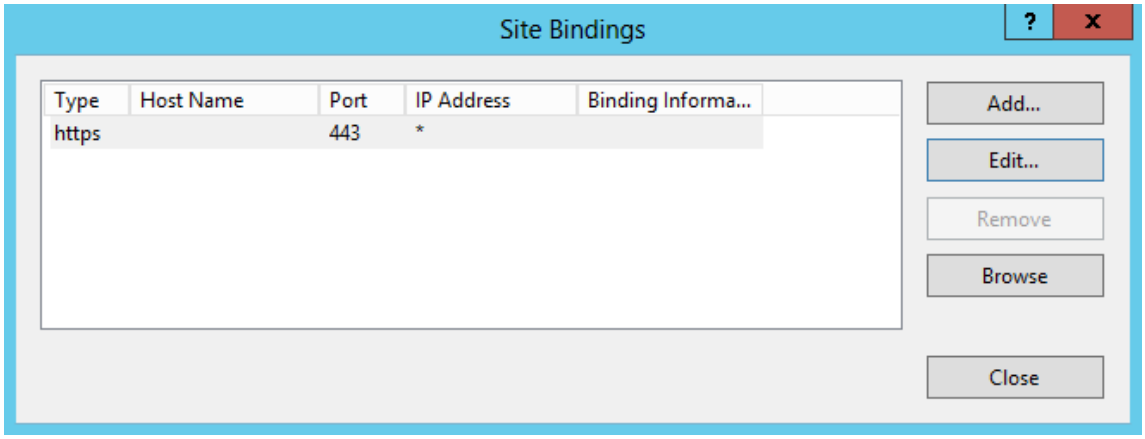
1. Cree un certificado adecuado para el servidor o grupo de servidores de StoreFront antes de instalar StoreFront.
2. Agregue el nombre de dominio completo compartido a los campos Nombre común y DNS. Compruebe que coincide con el nombre de dominio completo utilizado en el certificado SSL enlazado al servidor virtual de Citrix Gateway que ha creado anteriormente o, si no, utilice el mismo certificado enlazado al servidor virtual de Citrix Gateway.
3. Agregue el alias de la cuenta (`accounts.example.com`) al certificado como otro nombre SAN. Tenga en cuenta que el alias de cuentas que se usa en SAN es el que se usa en el perfil de sesión de Citrix Gateway en el procedimiento anterior: **Perfil y directiva de sesiones de puerta de enlace de Receiver nativo**.



4. Compruebe que la clave privada se puede exportar para que el certificado se pueda transferir a otro servidor de StoreFront o a varios nodos de un grupo de servidores de StoreFront.

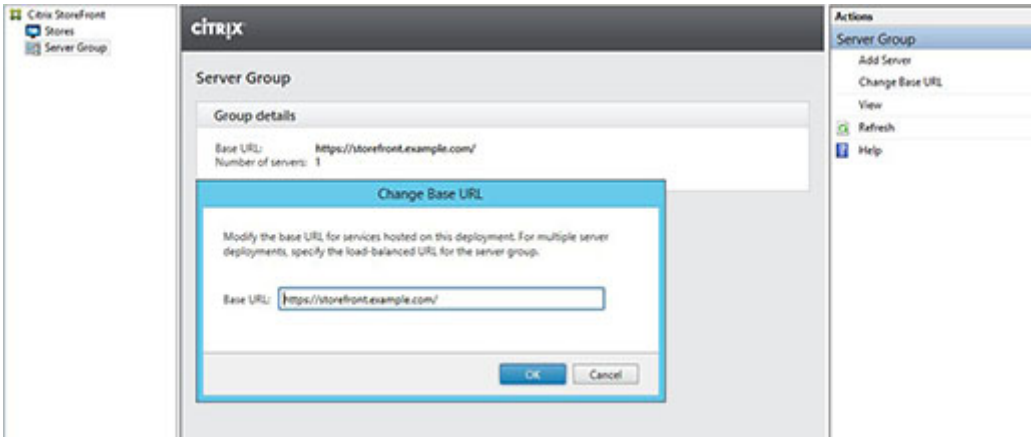


5. Firme el certificado con una entidad de certificación de terceros, como VeriSign, una CA raíz de la empresa o un certificado CA de intermedios.
6. Exporte el certificado en formato PFX e incluya la clave privada.
7. Importe el certificado y la clave privada en el servidor de StoreFront. Si va a implementar un clúster de StoreFront de Windows sin equilibrio de carga, importe el certificado en todos los nodos. Si utiliza otro equilibrador de carga, como, por ejemplo, un servidor virtual de Citrix ADC con equilibrio de carga, importe el certificado ahí en su lugar.
8. Cree un enlace HTTPS de IIS en el servidor de StoreFront y enlácele el certificado SSL importado.



9. Configure la URL base del host en el servidor de 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 `HTTPS://<FQDN>` válida, siempre que exista en el certificado como un nombre SAN. Ejemplo: `https://storefront.example.com`.



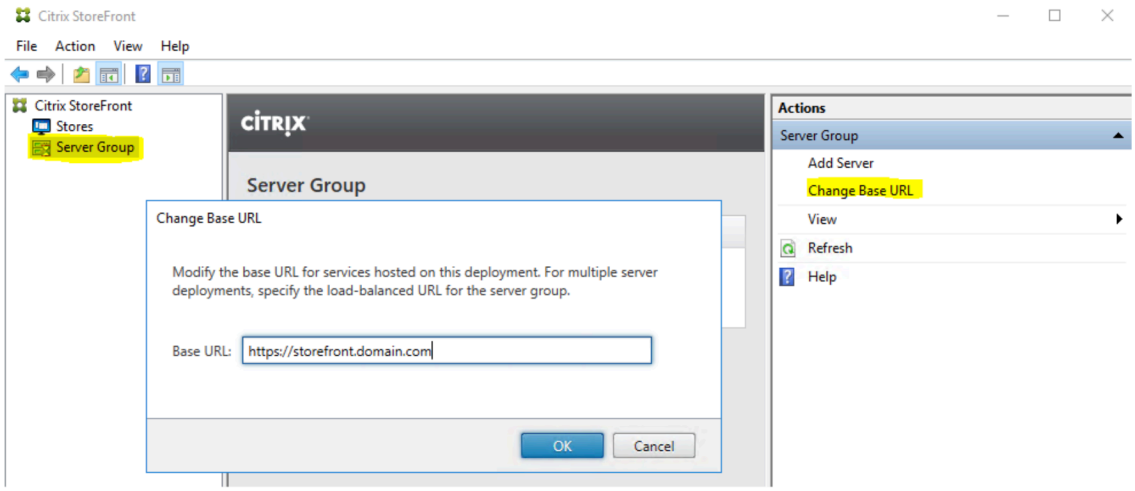
Cambiar la dirección URL base del servidor de HTTP a HTTPS

La opción URL base de host está disponible al configurar la implementación de servidor único o la implementación de un grupo de servidores en Citrix StoreFront. Esto se aplica a los clientes que hayan instalado y configurado Citrix StoreFront sin un certificado de servidor. Después de instalar el certificado, asegúrese de que StoreFront y sus servicios utilicen una conexión segura para continuar.

> Nota:
>
> El administrador de TI debe generar e instalar un certificado de servidor en el servidor Citrix StoreFront antes de ejecutar este procedimiento. Además, se debe crear un vínculo IIS a través de HTTPS (443) para proteger cualquier conexión nueva.

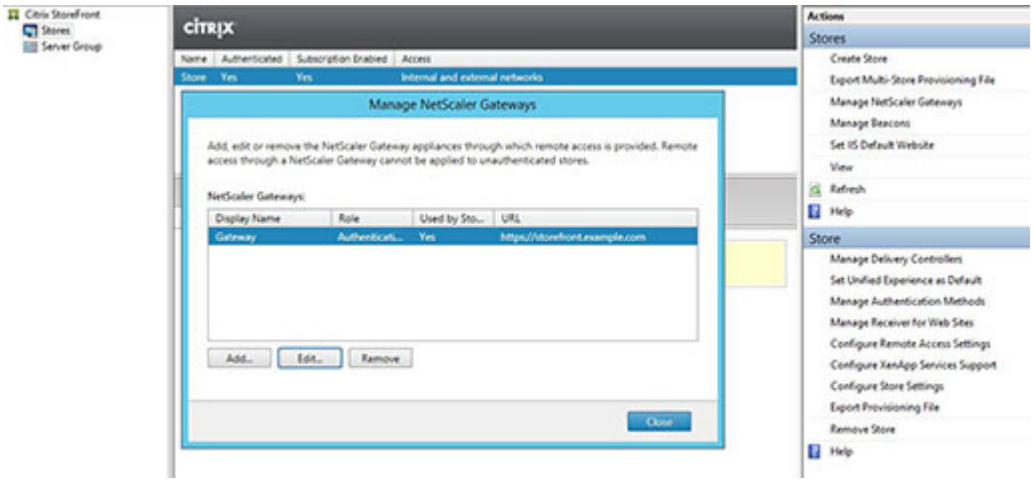
Complete los siguientes pasos para cambiar la URL base en StoreFront 3.x:

1. En StoreFront, haga clic en **Grupo de servidores** en el panel izquierdo.
2. Haga clic en **Cambiar URL base** en el panel derecho.
3. Escriba la dirección URL base y haga clic en **Aceptar**.

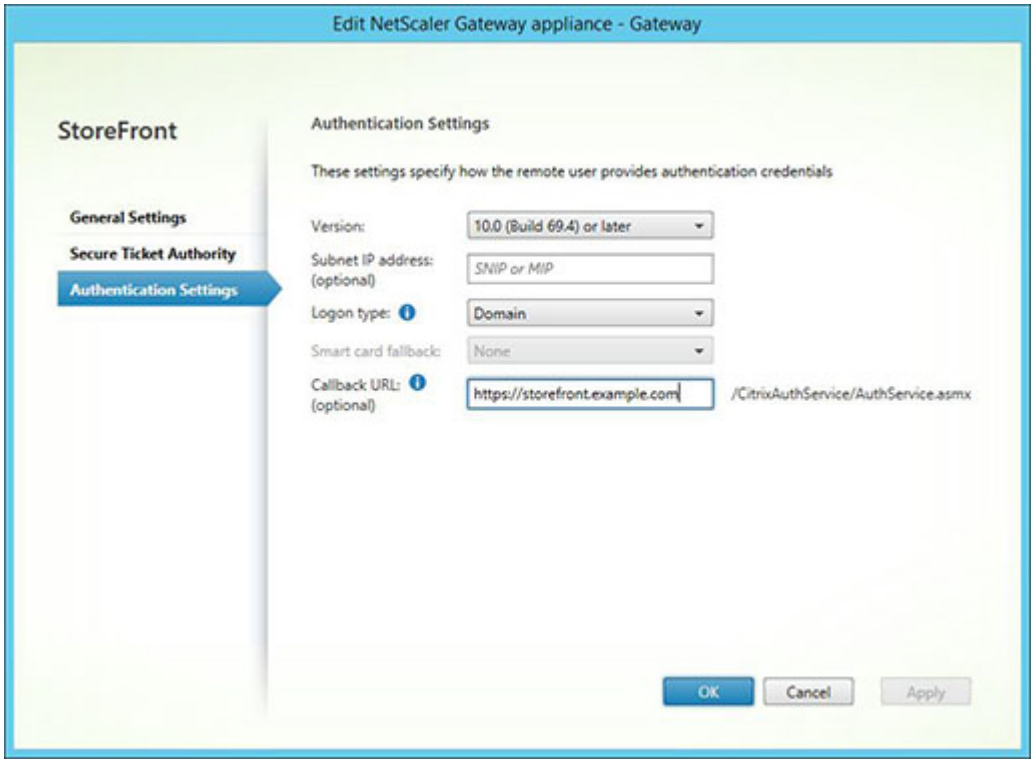


Configurar Gateway en el servidor de StoreFront: storefront.example.com

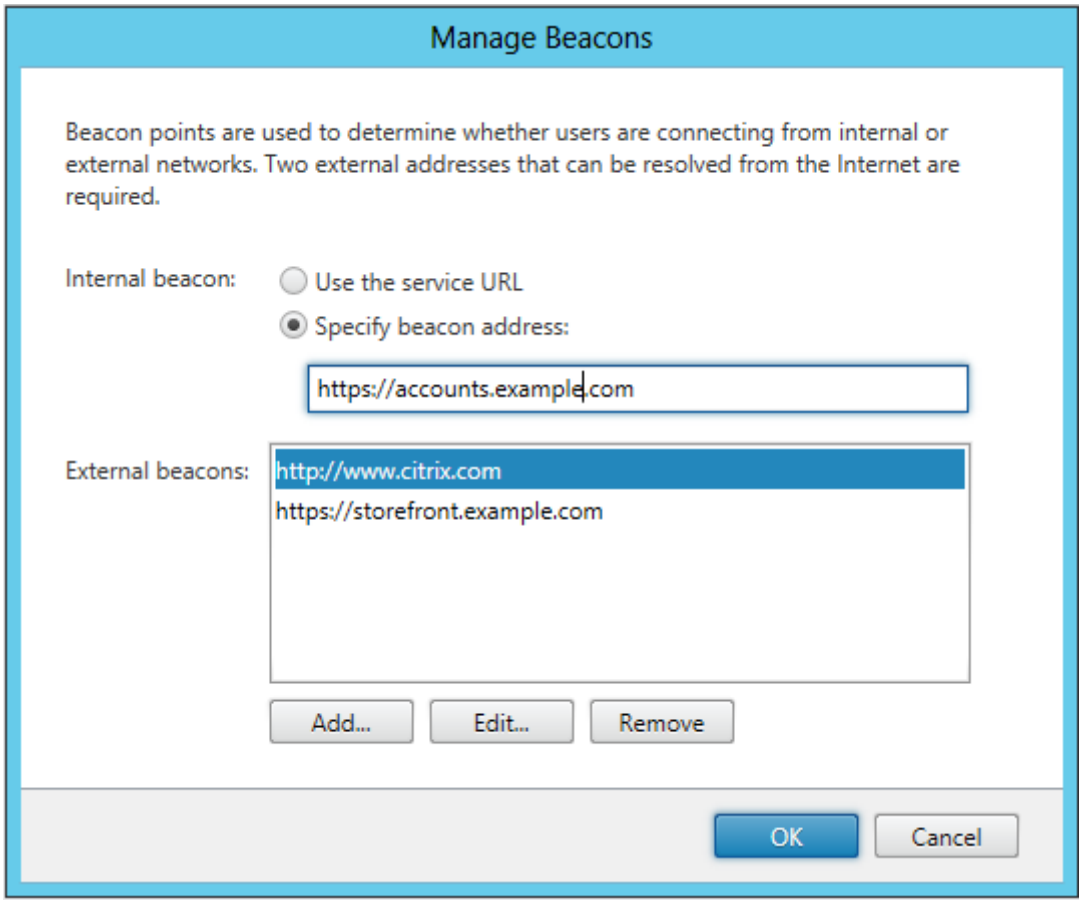
1. En el nodo **Almacenes**, haga clic en **Administrar dispositivos Citrix Gateway** en el panel **Acciones**.
2. Seleccione **Gateway** en la lista y haga clic en **Modificar**.



3. En la página **Parámetros generales**, introduzca el nombre de dominio completo compartido en el campo **URL de Citrix 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 **Almacén**.
6. Habilite el acceso remoto al almacén.
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 Citrix 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.



Habilitar la detección mediante nombres de dominio completo

Para habilitar 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 <allowedAudiences> adicional en *C:\inetpub\wwwroot\Citrix\Authentication\web.config*. Hay dos entradas <allowedAudiences> en este archivo. Solo la primera entrada del archivo requiere agregar una entrada <allowedAudience> más para el productor de tokens de autenticación.

1. En la sección <service id>, busque la cadena <allowedAudiences>. Agregue una línea para audience="https://accounts.example.com/", como se muestra aquí. guardar y cerrar el archivo web.config.

```
<service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="
    Authentication Token Producer">
...
<allowedAudiences>
<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
```

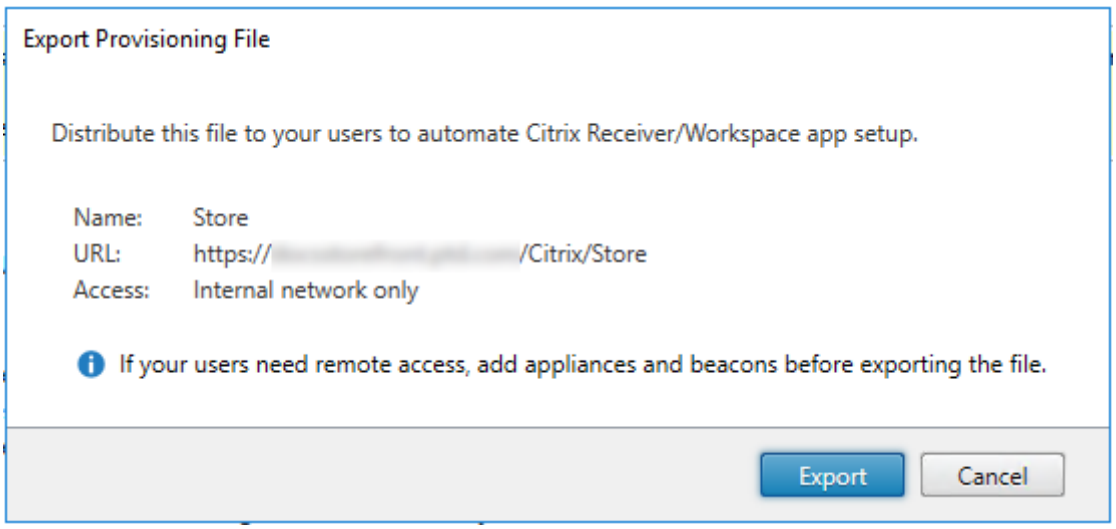


```
<add name="https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
```

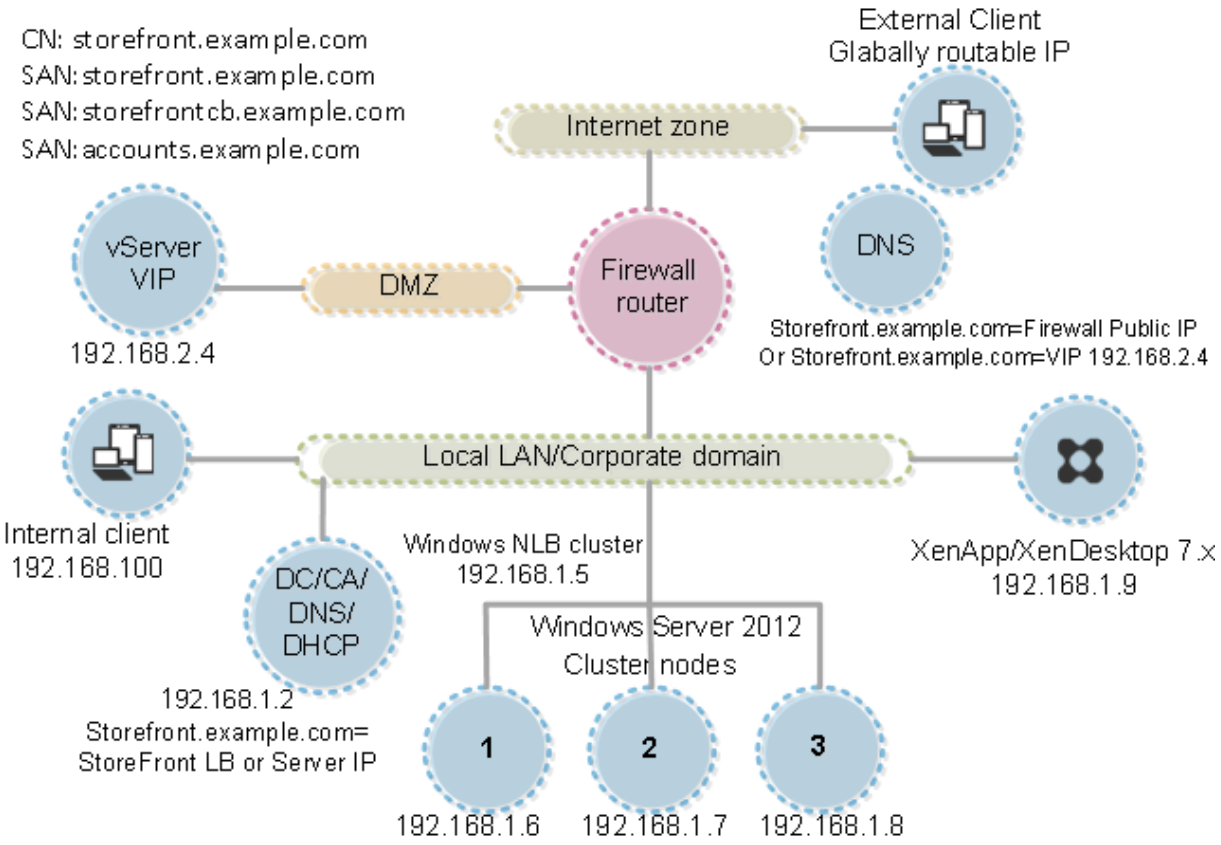
2. En *C:\inetpub\wwwroot\Citrix\Roaming\web.config*, busque la sección <tokenManager> y agregue una línea para `audience="https://accounts.example.com/"`, como se muestra aquí. guardar y cerrar el archivo web.config.

```
<tokenManager>
<services>
<clear />
...
</trustedIssuers>
<allowedAudiences>
<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
<add name='https-accounts.example.com" audience="https://accounts.
    example.com/" />
</allowedAudiences>
</service>
</services>
</tokenManager>
```

También puede exportar el archivo CR de aprovisionamiento del Receiver nativo para el almacén. Así, ya no es necesario configurar el primer uso de la aplicación Citrix Workspace. Distribuya este archivo a todos los clientes con aplicaciones Citrix Workspace en Windows y Mac.



Si ya hay una aplicación Citrix Workspace instalada en el cliente, el tipo de archivo CR se reconoce y, al hacer doble clic en el archivo de aprovisionamiento, se inicia la importación.



Configuraciones avanzadas

January 6, 2020

Puede configurar la siguiente opción avanzada desde la consola de StoreFront, PowerShell, propiedades de certificado o archivos de configuración.

Tarea	Detalles
Configurar el filtrado de recursos	Puede filtrar recursos de enumeración según el tipo de recurso y las palabras clave.

Configurar el filtrado de recursos

December 23, 2019

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 almacenes. 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 obtener más información, consulte la Módulos de PowerShell del SDK de Citrix StoreFront.

> Nota:
>
> 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.

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 Citrix Virtual Apps and Desktops. 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:

- Auto (Automático)
- Mandatory (Obligatorio)

Para obtener más información sobre palabras clave, consulte Optimizar la experiencia de usuario y Configurar la entrega de aplicaciones.

Ejemplos

Este comando utiliza el filtrado para excluir recursos de flujos de trabajo presentes en la enumeración:

```
1 Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -
    ExcludeKeywords @("WFS")
```

Este ejemplo aplica los tipos permitidos de recurso solo a aplicaciones:

```
1 Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -
    IncludeTypes @("Applications")
```

Configurar mediante archivos de configuración

January 6, 2020

Puede utilizar archivos de configuración para definir parámetros adicionales de Citrix StoreFront y Citrix Receiver para Web que no pueden establecerse con la consola de administración de Citrix StoreFront.

Puede configurar los siguientes parámetros de Citrix StoreFront:

- Habilitar ICA File Signing
- Inhabilitar la asociación de tipos de archivo
- Personalizar el cuadro de diálogo de inicio de sesión de la aplicación Citrix Workspace

- Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario

Puede configurar los siguientes parámetros de Citrix Receiver para Web:

- Cómo se muestran los recursos a los usuarios
- Inhabilitar la vista de carpetas de Mis aplicaciones

Configurar StoreFront mediante los archivos de configuración

January 6, 2020

En este artículo se describen las tareas de configuración adicionales que no se pueden llevar a cabo con la consola de administración de Citrix StoreFront.

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

Habilitar ICA File Signing

StoreFront ofrece la opción de firmar digitalmente los archivos ICA para que las versiones de la aplicación Citrix Workspace 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 de StoreFront. Los archivos ICA pueden firmarse con cualquier algoritmo hash compatible con el sistema operativo que se ejecuta en el servidor de 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, esto debe permitir que la clave se use para 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 los almacenes. Para activar la función ICA File Signing, modifique el archivo de configuración del almacén y ejecute comandos de Windows PowerShell. Para obtener más información sobre cómo habilitar ICA File Signing en la aplicación Citrix Workspace, consulteProtección ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza con ICA File Signing.

> Nota:
>
> 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. Asegúrese de que el certificado que quiere usar para firmar los archivos ICA esté disponible en el almacén de certificados de Citrix Delivery Services en el servidor de StoreFront y no en el almacén de certificados del usuario actual.
2. Utilice un editor de texto para abrir el archivo web.config del almacén (suele estar en el directorio C:\inetpub\wwwroot\Citrix\storename\), donde storename es el nombre especificado para el almacén durante su creación.
3. Busque la siguiente sección en el archivo.

```
<certificateManager>
    <certificates>
        <clear />
        <add ... />
        ...
    </certificates>
</certificateManager>
```

4. Incluya los detalles del certificado que se utilizarán para la firma.

```
<certificateManager>
    <certificates>
        <clear />
        <add id="certificateid" thumb="certificatethumbprint" />
        <add ... />
    ...
    </certificates>
```



```
</certificateManager>
```

Donde **certificateid** es un valor que le ayudará a identificar el certificado en el archivo de configuración del almacén 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.

```
<icaFileSigning enabled="False" certificateId="" hashAlgorithm="
    sha1" />
```

6. Cambie el valor del atributo habilitado a True para habilitar la firma ICA File Signing para el almacén. 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 distinto de SHA-1, establezca el valor del atributo hashAgorithm en sha256, sha384 o sha512, según sea necesario.
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 que el almacén acceda a la clave privada.

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
  $certificate = Get-DSCertificate "certificatethumbprint"
Add-DSCertificateKeyReadAccess -certificate $certificates[0] -
    accountName "IIS APPPOOL\Citrix Delivery Services Resources"
```

Donde certificatethumbprint es el resultado de los datos del certificado generado por el algoritmo hash.

Inhabilitar la asociación de tipos de archivo

De forma predeterminada, la asociación de tipos de archivo está habilitada en los almacenes para que el contenido se redirija directamente a las aplicaciones suscritas de los usuarios cuando estos abran archivos locales de los correspondientes tipos. Para inhabilitar la asociación de tipos de archivo, modifique el archivo de configuración del almacén.

1. Utilice un editor de texto para abrir el archivo web.config del almacén (suele estar en el directorio C:\inetpub\wwwroot\Citrix\storename\), donde storename es el nombre especificado para el almacén durante su creación.
2. Localice el siguiente elemento en el archivo.

```
<farmset ... enableFileTypeAssociation="on" ... >
```


3. Cambie el valor del atributo enableFileTypeAssociation a off para inhabilitar la asociación de tipos de archivo para el almacén.

Personalizar el cuadro de diálogo de inicio de sesión de la aplicación Citrix Workspace

De forma predeterminada, cuando los usuarios inician sesión en un almacén, 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 del título en el cuadro de diálogo de inicio de sesión, modifique los archivos del servicio de autenticación.

1. Utilice un editor de texto para abrir el archivo UsernamePassword.tfrm del servicio de autenticación (suele estar en el directorio C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\).
2. Busque las siguientes líneas en el archivo.

```
@* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
```

3. Quite la marca de comentario de la instrucción eliminando los elementos iniciales y finales **@*** y ***@**.

```
@Heading("ExplicitAuth:AuthenticateHeadingText")
```

   Los usuarios de la aplicación Citrix Workspace ven el texto de título predeterminado "Please log on" o la versión localizada de este texto cuando inician sesión en los almacenes donde se utiliza este servicio de autenticación.

4. Para modificar el texto de título, utilice un editor de texto para abrir el archivo *ExplicitFormsCommon.xx.resx* del servicio de autenticación (suele estar en el directorio C:\inetpub\wwwroot\Citrix\Authentication\App_Data\resources\).
5. Localice los siguientes elementos en el archivo. Modifique el texto escrito dentro del elemento <value> para modificar el texto del título que los usuarios ven en el cuadro de diálogo de inicio de sesión al acceder a almacenes en los que se utiliza este servicio de autenticación.

```
<data name="AuthenticateHeadingText" xml:space="preserve">
    <value>My Company Name</value>
</data>
```

   Para modificar el texto de título del cuadro de diálogo de inicio de sesión para los usuarios con otras configuraciones regionales, modifique los archivos *ExplicitAuth.languagecode.resx* traducidos, donde **languagecode** es el identificador de configuración regional.

Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario

De manera predeterminada, la aplicación Citrix Workspace para Windows almacena las contraseñas de los usuarios cuando inician sesión en los almacenes de StoreFront. Para evitar que Citrix Receiver para Windows o la aplicación Citrix Workspace para Windows, pero no Citrix Receiver para Windows Enterprise, almacene en caché las contraseñas de los usuarios, modifique los archivos del servicio de autenticación.

1. Use un editor de texto para abrir el archivo inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePassword.tfrm.
2. Busque la siguiente línea en el archivo.

```
1 @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
```

3. Comente la instrucción como se muestra a continuación.

```
1 <!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",
    initiallyChecked: ControlValue("SaveCredentials")) -->
```

   Los usuarios deben introducir sus contraseñas cada vez que inician sesión en almacenes 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. Haga una copia de seguridad del Registro antes de modificarlo.

De manera predeterminada, Citrix Receiver para Windows rellena el formulario automáticamente con el último nombre de usuario que se utilizó. Para que el campo de nombre de usuario no se rellene previamente, modifique el Registro en el dispositivo del usuario:

1. Cree un valor REG_SZ HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Establezca su valor en “false”.

Configurar sitios de Citrix Receiver para Web mediante los archivos de configuración

July 25, 2019

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.

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

Configurar cómo se muestran los recursos a 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. Lo primero que ven los usuarios es el escritorio 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, modifique el archivo de configuración del sitio.

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 del almacén en el momento de su creación.
2. Localice el siguiente elemento en el archivo.

```
1 <uiViews showDesktopsView="true" showAppsView="true" defaultView="
    desktops" />
```

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 estén disponibles en 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.


```
<userInterface ... autoLaunchDesktop="true">
```

5. Cambie el valor del atributo **autoLaunchDesktop** a **false** para evitar que los sitios de Citrix Receiver 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.

Inhabilitar la vista de carpetas de Mis aplicaciones

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 del almacén en el momento de su creación.
2. Localice el siguiente elemento en el archivo.

```
<userInterface enableAppsFolderView="true">
```

3. Cambie el valor del atributo **enableAppsFolderView** a **false** para inhabilitar la vista de la carpeta Mis aplicaciones en Citrix Receiver para Web.

Proteger la implementación de StoreFront

March 2, 2020

En este artículo se muestran las áreas que pueden afectar la seguridad del sistema durante la implementación y la configuración de StoreFront.

Configurar Microsoft Internet Information Services (IIS)

StoreFront puede configurarse con una configuración restringida de IIS. Esta no es la configuración predeterminada de IIS.

Extensiones de nombre de archivo

Puede prohibir extensiones de nombre de archivo no incluidas en la lista.

StoreFront requiere las siguientes 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
- .txt
- .xml

Si la descarga o la actualización de la aplicación Citrix Workspace está habilitada para Citrix Receiver para Web, StoreFront también requiere estas extensiones de nombre de archivo:

- .dmg
- .exe

Si la aplicación Citrix Workspace para HTML5 está habilitada, StoreFront también requiere estas extensiones de nombre de archivo:

- .eot
- .ttf
- .woff

Tipos MIME

Puede quitar tipos MIME que correspondan a los siguientes tipos de archivo:

- .exe
- .dll
- .com

- .bat
- .csh

Filtrado de solicitudes

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

Otros parámetros de Microsoft IIS

StoreFront no requiere:

- Filtros de ISAPI
- Extensiones ISAPI
- Programas CGI
- Programas FastCGI

> **Importante:**
>
> - No configure reglas de autorización de IIS. StoreFront admite la autenticación directamente y no utiliza ni admite la autenticación de IIS.
> - No seleccione **Certificados de cliente: Requerir**, en los parámetros de SSL para el sitio de StoreFront. La instalación de StoreFront configura las páginas apropiadas del sitio de StoreFront con este parámetro.
> - StoreFront requiere cookies. Debe seleccionar el parámetro Usar cookies. No seleccione el Modo sin cookies/Usar URI.
> - StoreFront requiere Plena confianza. No configure el nivel de confianza de .NET con un nivel Alto o inferior.
> - StoreFront no admite el uso de grupos de aplicaciones separados para cada sitio. No modifique estos parámetros de sitio. No obstante, puede establecer el tiempo de espera de inactividad y la cantidad de memoria virtual que usa la agrupación de aplicaciones.

Configurar derechos de usuario

> Nota:
>
> Microsoft IIS está habilitado como parte de la instalación de StoreFront. Microsoft IIS concede el derecho de inicio de sesión **Iniciar sesión como proceso por lotes** y el privilegio **Suplantar**

> **un cliente después de la autenticación** en el grupo integrado IIS_IUSRS. Este es el comportamiento normal de instalación de Microsoft IIS. No cambie estos derechos de usuario. Consulte la documentación de Microsoft para obtener más información.

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. Los grupos de aplicaciones son Citrix Configuration API, Citrix Delivery Services Resources, Citrix Delivery Services Authentication, y Citrix Receiver para Web.

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.

Configurar 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); no cambie esta configuración. El servicio Citrix StoreFront Protocol Transition inicia sesión como SYSTEM (Sistema); no cambie esta configuración.

Configurar la pertenencia a grupos

Al configurar un grupo de servidores de StoreFront, se agregan los siguientes servicios al grupo de seguridad Administradores:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService). Este servicio solo es visible en servidores que forman parte de un grupo y solo se ejecuta mientras la unión está en curso.

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 la aplicación Citrix Workspace en un dispositivo, debe instalar un certificado de servidor válido en el servidor de 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 del tipo Sujeto o Nombre alternativo del sujeto de **discoverReceiver.dominio**, donde dominio 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 la aplicación Citrix Workspace se conecte por primera vez al servidor de 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 Configurar la detección de cuentas basada en direcciones de correo electrónico.

Si los usuarios configuran sus cuentas mediante las direcciones URL del almacén directamente en la aplicación Citrix Workspace y no usan la detección de cuentas basada en direcciones de correo electrónico, el certificado del servidor de 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 los almacenes requieren certificados para la administración de tokens. StoreFront genera un certificado autofirmado cuando se crean servicios de autenticación o almacenes. 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 de 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 un almacén 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 <*directorio de instalación*>\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 admita la directiva de

ejecución de PowerShell. Recomendamos usar la directiva **AllSigned**. (La directiva **Restringida** no se admite, ya que impide la ejecución de scripts de PowerShell.) StoreFront no altera 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 haya 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 Citrix Virtual Apps. El Traspaso SSL es un componente predeterminado de Citrix Virtual Apps que lleva a cabo la autenticación del host y el cifrado de datos.

Citrix recomienda inhabilitar la compatibilidad con TLS 1.0 y 1.1 en el servidor web que aloja StoreFront. Debe aplicarlo a través de objetos de directiva de grupo, que crean los parámetros del Registro necesarios en el servidor de StoreFront para inhabilitar protocolos anteriores, como TLS 1.0 y TLS 1.1. Consulte también el apartado Configuración de TLS/SSL de Microsoft como referencia.

Citrix recomienda proteger la comunicación entre los dispositivos de los usuarios y StoreFront mediante Citrix Gateway y HTTPS. Para utilizar HTTPS, StoreFront requiere que la sesión de Microsoft Internet Information Services (IIS) que aloja el servicio de autenticación y los almacenes asociados 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.

Separar la 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.

Entrega de aplicaciones web y SaaS a través de Storefront

Puede entregar de forma segura sus aplicaciones web y SaaS a los usuarios a través de su almacén StoreFront. Con Citrix Cloud y la utilidad Access Control Sync for StoreFront, puede emplear directivas mejoradas de seguridad y filtrado web para estas aplicaciones a fin de proteger a sus usuarios y la red de malware y fugas de datos. Los usuarios acceden a su almacén de StoreFront como de costumbre para iniciar las aplicaciones web y SaaS que haya configurado en Citrix Cloud. Para obtener más información, consulte Control de acceso para aplicaciones web y SaaS en StoreFront.

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 la aplicación Citrix Workspace 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 de StoreFront, incluidos SHA-1 y SHA-256. Para obtener más información, consulte Habilitar ICA File Signing.

Cambio de contraseña por parte de los usuarios

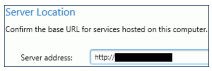
Puede permitir el cambio de contraseñas por parte de los usuarios de los sitios de Receiver para Web que inicien sesión con credenciales de dominio de Active Directory. Una vez concedido el permiso, los usuarios podrán cambiarlas en cualquier momento o solo cuando hayan caducado. No obstante, esto deja funciones de seguridad importantes al alcance de cualquier persona que pueda acceder a los almacenes 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 los almacenes 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 Optimizar la experiencia de usuario.

Cambiar la dirección URL base del servidor de StoreFront de HTTP a HTTPS

Para utilizar HTTPS para proteger la comunicación entre StoreFront y los dispositivos de los usuarios, debe configurar Microsoft Internet Information Services (IIS) para HTTPS. Si instala y configura Citrix StoreFront sin instalar y configurar primero un certificado SSL, StoreFront utiliza HTTP para las comunicaciones.

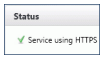
Si instala y configura un certificado SSL más adelante, utilice el siguiente procedimiento para asegurarse de que StoreFront y sus servicios utilizan conexiones HTTPS.

Ejemplo:



Antes de cambiar la URL base a HTTPS:

Después de cambiar la URL base a HTTPS:



1. Configure Microsoft Internet Information Services (IIS) para HTTPS en el servidor de StoreFront:
   a) Utilice la consola del administrador de Internet Information Services (IIS) para importar un certificado de servidor SSL firmado por la entidad de certificación del dominio de Microsoft Active Directory.
   b) Agregue un enlace de IIS sobre HTTPS (443) al sitio web predeterminado.

   Para obtener instrucciones detalladas, consulte CTX200292.
2. En la consola de administración de Citrix StoreFront, en el panel izquierdo seleccione **Grupo de servidores**.
3. En el panel Acciones, seleccione **Cambiar URL base**.
4. Escriba la dirección URL base y haga clic en **Aceptar**.

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.

Información adicional de seguridad

> **Nota:**
>
> Esta información puede cambiar en cualquier momento y sin previo aviso.

Es posible que su organización quiera realizar análisis de seguridad de StoreFront por motivos normativos. Las opciones de configuración anteriores pueden ayudar a eliminar algunos hallazgos en los informes de análisis de seguridad.

Si hay una puerta de enlace entre el analizador de seguridad y StoreFront, algunos hallazgos pueden estar relacionados con la puerta de enlace en lugar de con StoreFront. Los informes de análisis de seguridad generalmente no distinguen estos hallazgos (por ejemplo, la configuración de TLS). Debido a esto, las descripciones técnicas de los informes de análisis de seguridad pueden ser engañosas.

Al interpretar los informes de análisis de seguridad, tenga en cuenta lo siguiente:

- Es posible que las páginas HTML de StoreFront no incluyan protección contra los secuestros de clics (por los encabezados de respuesta de Content Security Policy o X-Frame-Options). Sin embargo, estas páginas HTML consisten solo en contenido estático y, por lo tanto, los ataques por secuestro de clics no son relevantes.
- La versión de Microsoft IIS y el uso de ASP.NET son visibles en los encabezados HTTP. Sin embargo, esta información ya se desprende de la presencia de StoreFront, ya que se basa en estas tecnologías.
- Al iniciar aplicaciones y escritorios, StoreFront utiliza un token para protegerse de la falsificación de solicitudes entre sitios (CSRF). Este token se envía como una cookie en una respuesta sin marcarse como seguro o solo HTTP. Cuando, posteriormente, se envía en una solicitud, el token se incluye en la cadena de la consulta de una URL. Sin embargo, StoreFront no confía en este mecanismo para autenticar las solicitudes HTTP.
- StoreFront utiliza el componente de código abierto jQuery. Una versión que se utiliza es jQuery 1.3.2. De acuerdo con el proyecto de código abierto jQuery, se realizó un cambio en jQuery 1.12.0 para mitigar posibles vulnerabilidades en una forma específica de solicitud entre dominios. Este cambio no mitigaba una vulnerabilidad en el propio jQuery; mitigaba el posible mal uso por lógica de aplicación. La lógica de aplicación de Citrix relevante, en la función de Receiver para Web compartida por NetScaler y StoreFront, no utiliza esta forma específica de solicitud entre dominios, no se ve afectada por esta vulnerabilidad y no se benefició de esta mitigación.

  Esta mitigación se eliminó posteriormente en jQuery 1.12.3 por razones de compatibilidad. Dado que la lógica de la aplicación de Citrix no se benefició de esta mitigación, esta eliminación no tiene ningún impacto material en las versiones de NetScaler y StoreFront con jQuery 1.12.4.

Exportar e importar la configuración de StoreFront

March 2, 2020

> Nota:
>
> Solo puede importar configuraciones de StoreFront que sean de la misma versión de StoreFront que la instalación de StoreFront de destino.

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 implementación con 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.

Escenarios en los que se puede utilizar la exportación e importación de configuraciones

- Solo implementaciones de copia de seguridad de StoreFront en un estado de confianza y funcionamiento correcto. Cualquier cambio en la configuración requiere que se realice una nueva copia de seguridad para reemplazar la anterior. No puede modificar las copias de seguridad existentes, ya que un hash del archivo backup.zip impide la modificación.
- Copia de seguridad ANTES de actualizar StoreFront a efectos de recuperación ante desastres.
- Clonación de implementaciones de prueba existentes de StoreFront para ponerlas en producción
- Creación de entornos de aceptación de usuarios mediante la clonación de implementaciones de producción en un entorno de prueba.
- Transferencia de StoreFront durante migraciones del sistema operativo, como la actualización del sistema operativo del host de 2008R2 a 2019.
- Creación de grupos de servidores adicionales en implementaciones para múltiples regiones, como en grandes empresas con varios centros de datos.

Aspectos a tener en cuenta al importar y exportar una configuración de StoreFront

- ¿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 admiten 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 mediante un objeto de credenciales de PowerShell 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.

Cmdlets de PowerShell

Export-STFConfiguration

Parámetro	Descripción
-TargetFolder <cadena>	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**.

Parámetro	Descripción
-ZipFileName <cadena>	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.

> **Importante:**
>
> El parámetro **-SiteID** de StoreFront 3.5 se retiró 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.NO se admite la importación de configuraciones de **SiteID 1** a **SiteID 2**.

Import-STFConfiguration

Parámetro	Descripción
-ConfigurationZip <cadena>	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. 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`

Parámetro	Descripción
-HostBaseURL <cadena>	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. Ejemplo:`https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

Parámetro	Descripción
-TargetFolder <cadena>	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 <cadena>	La ruta completa del archivo de copia de seguridad cifrado que quiere descifrar. Debe especificar la extensión de archivo .ctxzip. Ejemplo:`$env:userprofile\\desktop\\backup.ctxzip`
-OutputFolder <cadena>	La ruta para crear una copia no cifrada (.zip) del archivo de copia de seguridad cifrado (.ctxzip). El archivo cifrado de copia de seguridad original se conserva para poder volver a utilizarlo. No especifique ningún nombre de archivo ni una extensión de archivo para la copia no cifrada. Ejemplo:`$env:userprofile\desktop\`

Parámetro	Descripción
-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 los cmdlets de StoreFront en la sesión actual de PowerShell

Abra el entorno ISE (Integrated Scripting Environment) de PowerShell en el servidor de StoreFront y ejecute:

```
1 $env:PSModulePath = [Entorno] ::getEnvironmentVariable ('PSModulePath',
      'Máquina')
2 $SDKModules = 'C:\Archivos de programa\Citrix\Receiver StoreFront\
     PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.
     Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -
     verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -
     verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.
     psd1" -verbose
```

Casos 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

Exporte la configuración del servidor del que quiere realizar una copia de seguridad.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
     zipFileName "backup" -NoEncryption
```

Copie el archivo backup.zip en una ubicación segura. Puede utilizar esta copia de seguridad para recuperación ante desastres a fin de restaurar el servidor a su estado anterior.


```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://storefront.ejemplo.com"
```

Realizar una copia de seguridad de una configuración existente en el servidor A y restaurarla en el servidor B para crear un clon de un servidor existente

Exporte la configuración del servidor del que quiere realizar una copia de seguridad.

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -NoEncryption
```

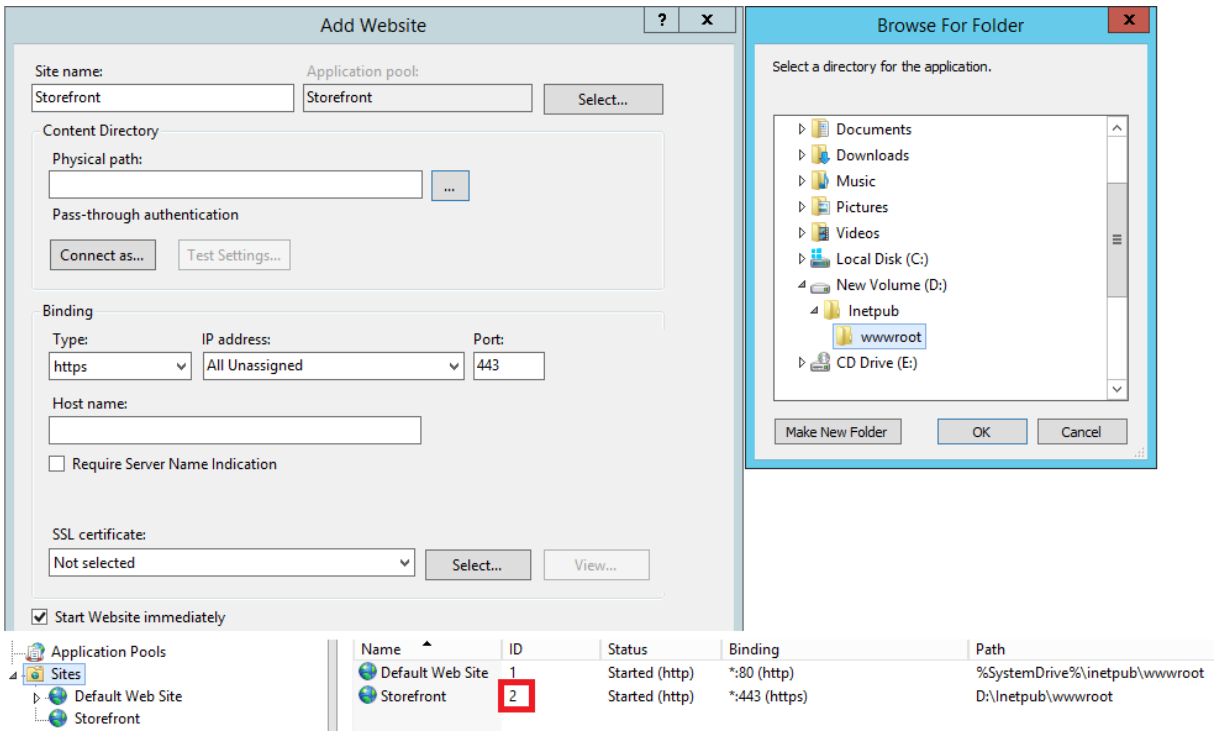
Copie el archivo backup.zip en el escritorio del servidor B.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.zip" -HostBaseURL "https://servidorB.ejemplo.com"
```

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. Exportar una copia de la configuración del servidor A.
2. En el Servidor B, configure IIS con un nuevo sitio web llamado **StoreFront**, que también usa **SiteID 2**.
3. Importar la configuración del Servidor A en el Servidor B. 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"-HostBaseURL "https://serverB.example.com"
```

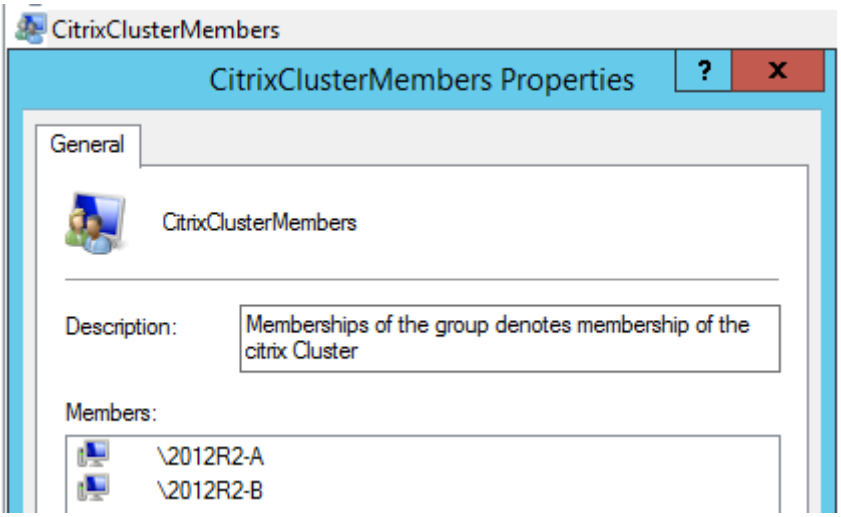
Casos de grupos de servidores

Caso 1: Hacer una copia de seguridad de la configuración de un grupo de servidores y restaurarla más tarde en la implementación del mismo grupo de servidores

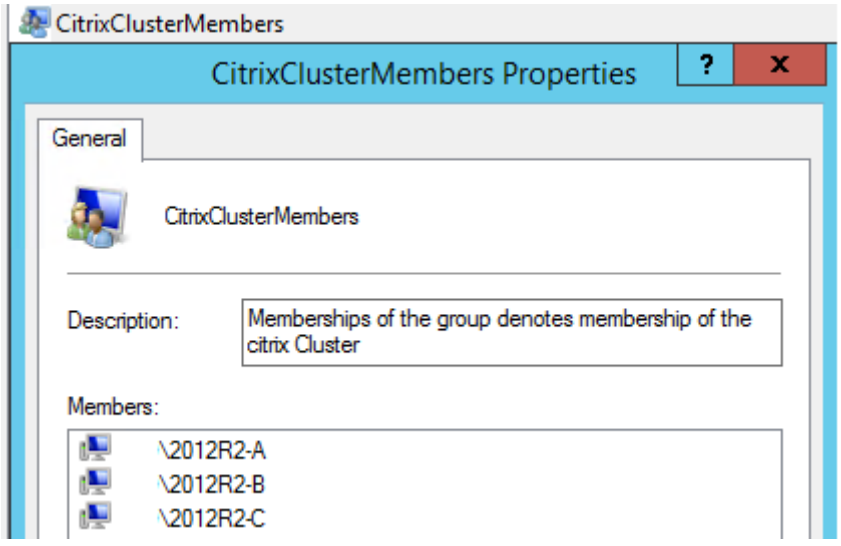
Anteriormente se hizo una copia de seguridad de la configuración, cuando el grupo de servidores solo tenía dos servidores de StoreFront, 2012R2-A y 2012R2-B. En el archivo de la copia de seguridad, dispone de un registro de **CitrixClusterMembership**. Este registro contiene el momento en el que se realizó la copia de seguridad con los dos servidores originales 2012R2-A y 2012R2-B. Posteriormente a la creación de esa copia de seguridad original, la implementación del grupo de servidores de 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 entrada 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 haya 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.



1. Más tarde, se agrega un servidor adicional, 2012R2-C al grupo de servidores existente.



1. 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.

2. Importe la configuración del grupo de servidores 1 de vuelta en el nodo 2012R2-A.

   ```
   Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
   backup.ctxzip"-HostBaseURL "https://servergroup1.example.com"
   ```

3. Propague la configuración recién importada en todo el grupo de servidores, de modo que los servidores tengan una configuración uniforme después de la importación.

Caso 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 con 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 con 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"-HostBaseURL "https://servergroup2.example.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.

Caso 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 del 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"-NoEncryption -HostBaseURL "https://servergroup2.example.
   com"
   ```

Crear una copia de seguridad cifrada de la configuración del servidor

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 la sesión 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 el usuario de Windows de la sesión actual.

Cree un objeto de credenciales de PowerShell dentro de su sesión de PowerShell en el servidor de exportación.

```
1 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
2 $Password = "Pa55w0rd"
3 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
4 $CredObject = New-Object System.Management.Automation.PSCredential(
     $User,$Password)
```

Exporte la configuración al archivo backup.ctxzip, que es un archivo zip cifrado.


```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
    zipFileName "backup" -Credential $CredObject
```

Cree un objeto de credenciales de PowerShell idéntico dentro de su sesión de PowerShell en el servidor de importación.

```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
    backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
    storefront.ejemplo.com"
```

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
```

SDK de StoreFront

January 6, 2020

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 ver la referencia del SDK, consulte SDK de StoreFront.

Diferencias principales entre el SDK de StoreFront 3.0 y el SDK de StoreFront actual

- **Ejemplos del SDK de alto nivel:** Esta versión proporciona scripts de SDK de alto nivel que le permiten automatizar las implementaciones de StoreFront rápida y fácilmente. 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, incluidos los almacenes, los métodos de autenticación, los sitios de Citrix Receiver para Web y los sitios unificados de Citrix Receiver, así como el acceso remoto a través de Citrix 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.

> **Importante:**
>
> 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 retirado 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 con una cuenta miembro del grupo de administradores locales en el servidor de 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 al 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 modificar 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
Crear una implementación simple	Script: crea una implementación simple de StoreFront con un controlador configurado con un único servidor XenDesktop.
Crear una implementación para acceso remoto	Script: Se basa en el script anterior y agrega acceso remoto a la implementación.
Crear una implementación para acceso remoto con una puerta de enlace óptima	Script: Se basa en el script anterior y agrega puertas de enlace preferidas óptimas para mejorar la experiencia del usuario.

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 con los métodos descritos para generar un script que automatice la imple-

mentación 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"
    )
    # Import StoreFront modules. Required for versions of
        PowerShell earlier than 3.0 that do not support
        autoloading
    Import-Module Citrix.StoreFront
    Import-Module Citrix.StoreFront.Stores
    Import-Module Citrix.StoreFront.Authentication
    Import-Module Citrix.StoreFront.WebReceiver
```

- Automatiza la ruta virtual de los servicios de autenticación y Citrix Receiver para Web basándose en la ruta **$StoreVirtualPath** proporcionada. **$StoreVirtualPath** equivale a **$StoreIISpath** porque las rutas virtuales siempre son la ruta de IIS. Por lo tanto, en PowerShell tienen un valor como "/Citrix/Store", "/Citrix/StoreWeb" o "/Citrix/StoreAuth".


```
# Determine the Authentication and Receiver virtual path to use
    based of the Store
$authenticationVirtualPath = "$($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 if the deployment already exists
$existingDeployment = Get-STFDeployment
if(-not $existingDeployment)
{

    # Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    # The deployment exists but it is configured to the desired
        hostbase url
    Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
 }

else
{

    Write-Error "A deployment has already been created on this
        server with a different host base url."
 }
```

- 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.

```
# Determine if the authentication service at the specified
    virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath
    $authenticationVirtualPath
if(-not $authentication)
{
```



```
5
6       # Add an Authentication service using the IIS path of the
            Store appended with Auth
7       $authentication = Add-STFAuthenticationService
            $authenticationVirtualPath
8    }
9
10  else
11  {
12
13      Write-Output "An Authentication service already exists at the
            specified virtual path and will be used."
14   }
```

- Crea un nuevo servicio de almacén configurado con un Controller de XenDesktop con los servidores en la matriz **$XenDesktopServers** en la ruta virtual especificada, si todavía no existe ninguna.

```
1   # Determine if the store service at the specified virtual path
        exists
2   $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3   if(-not $store)
4   {
5
6   # Add a Store that uses the new Authentication service configured
        to publish resources from the supplied servers
7   $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
        AuthenticationService $authentication -FarmName $Farmtype -
        FarmType $Farmtype -Servers $FarmServers -LoadBalance
        $LoadbalanceServers `
8           -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
                $TransportType
9    }
10
11  else
12  {
13
14      Write-Output "A Store service already exists at the specified
            virtual path and will be used. Farm and servers will be
            appended to this store."
15      # Get the number of farms configured in the store
16      $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
            Count
17      # Append the farm to the store with a unique name
18      Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
```



```
            $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
             -LoadBalance $LoadbalanceServers -Port $Port '
19           -SSLRelayPort $SSLRelayPort -TransportType $TransportType
20   }
```

- Agrega un servicio de Citrix Receiver para Web en la ruta virtual de IIS especificada para obtener acceso a las aplicaciones publicadas en el almacén creado anteriormente.

```
1  # Determine if the receiver service at the specified virtual path
       exists
2  $receiver = Get-STFWebReceiverService -VirtualPath
      $receiverVirtualPath
3  if(-not $receiver)
4  {
5
6      # Add a Receiver for Web site so users can access the
          applications and desktops in the published in the Store
7      $receiver = Add-STFWebReceiverService -VirtualPath
          $receiverVirtualPath -StoreService $store
8   }
9
10 else
11 {
12
13     Write-Output "A Web Receiver service already exists at the
          specified virtual path and will be used."
14  }
```

- Habilita XenApp Services para el almacén de modo que las versiones anteriores de clientes de Citrix Receiver o de la aplicación Citrix Workspace puedan conectarse a las aplicaciones publicadas.

```
1  # Determine if PNA is configured for the Store service
2  $storePnaSettings = Get-STFStorePna -StoreService $store
3  if(-not $storePnaSettings.PnaEnabled)
4  {
5
6  # Enable XenApp services on the store and make it the default for
       this server
7  Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
      -DefaultPnaService
8   }
```


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 con 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

# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
# Import StoreFront modules. Required for versions of PowerShell earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
```

- Cree una implementación de StoreFront de acceso interno ejecutando los scripts de los ejemplos anteriores. La implementación básica se ampliará para ofrecer el acceso remoto.

```
# Create a simple deployment by invoking the SimpleDeployment example
$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition -Parent
$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `
 -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort $SSLRelayPort -TransportType $TransportType
```

- Obtiene los servicios creados en la implementación sencilla porque tienen que actualizarse para admitir el caso de acceso remoto.

```
# Determine the Authentication and Receiver sites based on the Store
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$authentication = Get-STFAuthenticationService -StoreService $store
$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- Habilita CitrixAGBasic en el servicio de Citrix Receiver para Web, requerido para el acceso remoto a través de Citrix Gateway. Obtiene el método de autenticación ExplicitForms y CitrixAGBasic de Citrix Receiver para Web de los protocolos admitidos.

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols
# Included for demonstration purposes as the protocol name can be used directly if known
```



```
$receiverMethods = Get-
    STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
 $_ -match "Explicit" -or $_ -match "CitrixAG"  }

# Enable CitrixAGBasic in Receiver for Web (required for remote
    access)
Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
    $receiverMethods
```

- Habilita CitrixAGBasic en el servicio de autenticación. Esto es necesario para el acceso remoto.

```
# Get the CitrixAGBasic authentication method from the protocols
    installed.
# Included for demonstration purposes as the protocol name can be
     used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
    Object {
 $_ -match "CitrixAGBasic"  }

# Enable CitrixAGBasic in the Authentication service (required
    for remote access)
Enable-STFAuthenticationServiceProtocol -AuthenticationService
    $authentication -Name $citrixAGBasic
```

- Agrega una nueva puerta de enlace de acceso remoto, lo que agrega la dirección IP de subred optativa y la registra con el almacén al que se va a acceder de forma remota.

```
# Add a new Gateway used to access the new store remotely
Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
# Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
$gateway = Get-STFRoamingGateway -Name $GatewayName
# If the gateway subnet was provided then set it on the gateway
    object
if($GatewaySubnetIP)
{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
 }

```



```
# Register the Gateway with the new Store
Register-STFStoreGateway -Gateway $gateway -StoreService $store -
    DefaultGateway
```

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, compruebe que sigue los pasos detallados en Introducción al SDK. Este ejemplo se puede personalizar con 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,
```



```
18      [Parameter(Mandatory=$true)]
19      [string[]]$GatewaySTAUrls,
20      [string]$GatewaySubnetIP,
21      [Parameter(Mandatory=$true)]
22      [string]$GatewayName,
23      [Parameter(Mandatory=$true)]
24      [Uri]$OptimalGatewayUrl,
25      [Parameter(Mandatory=$true)]
26      [string[]]$OptimalGatewaySTAUrls,
27      [Parameter(Mandatory=$true)]
28      [string]$OptimalGatewayName
29  )
30  Set-StrictMode -Version 2.0
31  # Any failure is a terminating failure.
32  $ErrorActionPreference = 'Stop'
33  $ReportErrorShowStackTrace = $true
34  $ReportErrorShowInnerException = $true
35  # Import StoreFront modules. Required for versions of PowerShell
        earlier than 3.0 that do not support autoloading
36  Import-Module Citrix.StoreFront
37  Import-Module Citrix.StoreFront.Stores
38  Import-Module Citrix.StoreFront.Roaming
```

- Llama al script de implementación de acceso remoto para configurar la implementación básica y agregarle el acceso remoto.

```
1  # Create a remote access deployment
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
       ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype `
5       -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType `
6       -GatewayUrl $GatewayUrl -GatewayCallbackUrl
           $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
           GatewayName $GatewayName
```

- Agrega la preferencia de puerta de enlace de inicio óptima y la obtiene de las puertas de enlace configuradas.

```
1  # Add a new Gateway used for remote HDX access to desktops and
       apps
```



```
$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -
    LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -
    SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
```

- Obtiene el servicio del almacén para usar la puerta de enlace óptima, registrarla y asignarla a inicios desde una comunidad especificada.

```
# Get the Store configured by SimpleDeployment.ps1
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
# Register the Gateway with the new Store for launch against all
    of the farms (currently just one)
$farmNames = @($store.FarmsConfiguration.Farms | foreach {
 $_.FarmName  }
)
Register-STFStoreOptimalLaunchGateway -Gateway $gateway -
    StoreService $store -FarmName $farmNames
```

Ejemplo: Intercambio de metadatos entre el proveedor de identidades y el proveedor de servicios (StoreFront) para la autenticación SAML

La autenticación de SAML se puede configurar en la consola de administración de StoreFront (consulte Configurar el servicio de autenticación) o mediante los siguientes cmdlets de PowerShell:

- 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 un almacén de StoreFront, llamado “Store”, con su servicio de autenticación dedicado, el punto final de metadatos será:

```
https://<storefront host>/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:

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://example.com/FederationMetadata/2007-06/FederationMetadata.xml

# If the metadata has already been download, use the following:
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.xml"
```

Ejemplo: Listar los metadatos y los puntos finales de ACS para un almacén especificado 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 un almacén especificado.

```
# 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 salida:

```
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
```

Solucionar problemas de StoreFront

January 6, 2020

Cuando StoreFront se instala o desinstala, el instalador de StoreFront crea los siguientes archivos de registros en el directorio *C:\Windows\Temp\StoreFront*. 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, los almacenes 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 los almacenes y de los sitios de Receiver para Web.

La consola de administración de Citrix StoreFront registra la información de rastreo automáticamente. De forma predeterminada, el rastreo 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. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completado,
> propague los cambios de configuración al grupo de servidores para que se actualicen los demás servidores de la implementación.

Para configurar la limitación de registros

1. Utilice un editor de texto para abrir el archivo *web.config* del servicio de autenticación, el almacén o el sitio de Receiver para Web, que normalmente se encuentran en los directorios C:\inetpub\wwwroot\Citrix\Authentication, C:\inetpub\wwwroot\Citrix\storename, and C:\inetpub\wwwroot\Citrix\storenameWeb\ respectivamente, donde storename es el nombre que se especificó para el almacén cuando se creó.
2. Localice el siguiente elemento en el archivo.

   ```
   <logger duplicateInterval=”00:01:00”duplicateLimit=”10”>
   ```

   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.

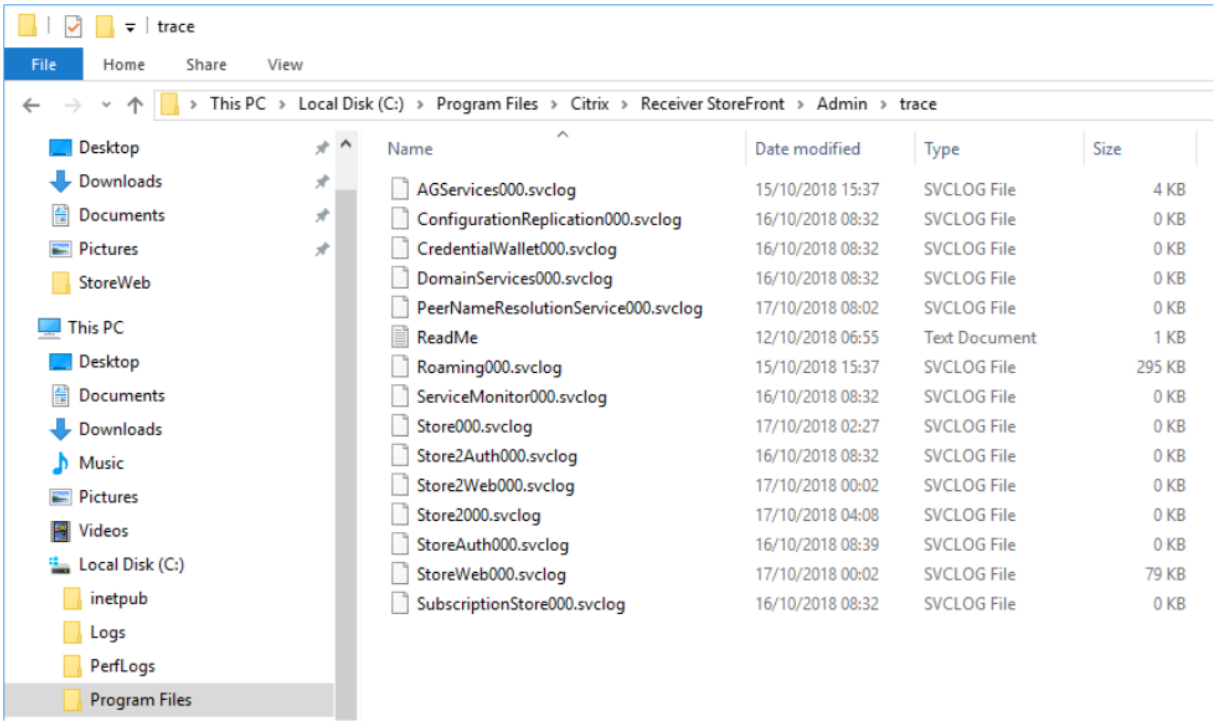
Cuando se inicie la limitación de registros, se registrará un mensaje de advertencia para indicar que se omitirán las entradas de registro posteriores que sean idénticas. Después de este límite de tiempo, se reanuda el registro normal y se registra un mensaje informativo que indica que las entradas de registro duplicadas ya no se omitirán.

Para habilitar el seguimiento para la depuración

> **Importante:**
>
> 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 consola de PowerShell

> antes de abrir la consola de StoreFront.

El rastreo resultante se envía a C:\Archivos de programa\Citrix\Receiver StoreFront\admin\trace



> **Nota:**
>
> Ejecute `Get-Help Set-STFDiagnostics -detailed` para obtener ayuda e instrucciones de PowerShell sobre cómo utilizar el cmdlet Set-STFDiagnostics.

Utilice una cuenta con permisos de administrador local para iniciar Windows PowerShell y, en el símbolo del sistema, escriba los siguientes comandos obligatorios para habilitar o inhabilitar el rastreo.

- **-All**. Un indicador de que el rastreo debe actualizarse en todas las instancias y servicios.
- **-TraceLevel**. Los valores permitidos para -TraceLevel son, en orden creciente de detalle de rastreo: Off, Error, Warning, Info, Verbose. Debido a la gran cantidad de datos que se pueden generar, el rastreo puede afectar significativamente al rendimiento de StoreFront. Los niveles Info o Verbose no se recomiendan, a menos que se requieran específicamente para la solución de problemas.

Parámetros opcionales:

- **-FileSizeKb**. El tamaño del archivo de rastreo en KB.
- **-FileCount**. Cantidad de archivos de rastreo que se deben mantener en el disco en un momento dado.
- **-confirm:$False**. Elimina las solicitudes de Windows para permitir que el cmdlet de StoreFront se ejecute cada vez.

Ejemplos

Para habilitar el rastreo de nivel Verbose (detallado) para todos los servicios con fines de depuración:

```
Set-STFDiagnostics -All -TraceLevel ”Verbose” -confirm:$False
```

Para inhabilitar el rastreo de nivel Verbose y volver a establecer el nivel de rastreo en el valor predeterminado para todos los servicios:

```
Set-STFDiagnostics -All -TraceLevel ”Error” -confirm:$False
```

Para obtener más información sobre el cmdlet Set-STFDiagnostics, consulte la documentación de StoreFront PowerShell SDK.

Para habilitar la captura de registros del archivo launch.ica

Guarde la información en el archivo launch.ica en el equipo cliente para solucionar diferentes problemas. Los servidores de la Interfaz Web o StoreFront generan el archivo launch.ica.

Para habilitar la captura de registros del archivo launch.ica, siga estos pasos:

1. Vaya a la siguiente clave de Registro mediante el Editor del Registro:

   En sistemas de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   En sistemas de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Establezca estos dos valores de clave de cadena:

   - LogFile=”ruta al archivo de registro”
   - LogICAFile=true

   Por ejemplo:

   ```
   LogFile=C:\ica\ica.log
   LogICAFile=true
   ```

Recursos adicionales

> Nota:
>
> El uso de un archivo ICA en el entorno para un fin que no sea la solución de problemas se describe más detalladamente en CTX200126.

Solucionar problemas de actualización de StoreFront

Siga estos pasos para solucionar problemas de actualización de StoreFront.

Antes de intentar una actualización

1. Confirme que tiene una copia de seguridad de todos los servidores de StoreFront.
2. Compruebe que no intenta actualizar StoreFront desde una versión de fin de vida. Para obtener más información, consulte CTX200356.
3. Compruebe que va a actualizar StoreFront solamente desde una versión compatible a la versión actual.
4. Si el servidor de StoreFront forma parte de un grupo de servidores de StoreFront, todos los servidores del grupo deben actualizarse secuencialmente. No se admite la actualización simultánea de un grupo de servidores de StoreFront.
5. Elimine los archivos *thumbs.db* que haya en *C:\inetpup\wwwroot\citrix* o en sus subdirectorios. Muestre los archivos ocultos para completar este paso: **Opciones de carpeta > Ver**, elija la opción **Mostrar archivos, carpetas y unidades ocultos** y desmarque la opción **Ocultar archivos protegidos del sistema operativo (recomendado)**.
6. Inhabilite el software antivirus antes de iniciar la actualización.
7. Confirme que los servidores que se van a actualizar se hayan quitado de los equilibradores de carga y que no tengan conectadas sesiones de usuario activas.
8. Reinicie el servidor de StoreFront antes de realizar la actualización.
9. Detenga manualmente los siguientes servicios:
    - CitrixConfigurationReplication
    - CitrixCredentialWallet
    - CitrixDefaultDomainService
    - CitrixPeerResolutionService
    - CitrixSubscriptionsStore
10. Asegúrese de que la consola de administración de StoreFront esté cerrada.

Si falla la actualización

1. En *C:\Windows\Temp\StoreFront*, abra el archivo *CitrixMsi*.log* más reciente y busque los errores de excepción que pueda haber.

    Excepciones del tipo **Thumbs.db Access**: Provocadas por los archivos *thumbs.db* que hay en *C:\inetpup\wwwroot\citrix* o en alguno de sus subdirectorios. Elimine los archivos *thumbs.db* que encuentre.

    Excepciones del tipo **Cannot get exclusive file access \in use**: Restaure la instantánea o copia de seguridad si está disponible, o bien reinicie el servidor y detenga manualmente los servicios

de StoreFront.

Excepciones del tipo **Service cannot be started**: Restaure la instantánea o copia de seguridad si está disponible, o bien instale la versión completa de .NET Framework 4.5 (no el perfil de cliente).

2. Si no hay errores de excepción en *CitrixMsi*.log*, compruebe **Visor de eventos > Delivery Services** en el servidor para ver si hay errores que contengan mensajes de los errores de excepción anteriores. Siga el consejo correspondiente.
3. Si no hay errores de excepción en el Visor de eventos, compruebe los registros de administración en *C:\Archivos de programa\Citrix\Receiver StoreFront\Logs* para ver si hay errores que contengan mensajes de los errores de excepción anteriores. Siga el consejo correspondiente.

Para quitar StoreFront manualmente

> Advertencia:
>
> El hecho de quitar StoreFront manualmente borra toda la información existente.

Para quitar StoreFront manualmente:

1. Desinstale StoreFront.
2. Quite el rol de servidor web.
3. Elimine la carpeta *C:\Archivos de programa\Citrix\Receiver StoreFront*.
4. Elimine cualquier subdirectorio de *C:\Archivos de programa\Citrix\StoreFront Install*.
5. Elimine la carpeta *C:\Inetpub*.

Ahora puede reinstalar StoreFront.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States