NetScaler Gateway 14.1

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Notas de versión de NetScaler Gateway

January 26, 2024

Las notas de la versión describen cómo ha cambiado el software en una compilación concreta y los problemas conocidos que existen en esa compilación.

El documento de notas de la versión incluye todas o algunas de las secciones siguientes:

- **Novedades**: Las mejoras y otros cambios publicados en la compilación.
- **Problemas solucionados**: Los problemas que se han solucionado en la compilación.
- **Problemas conocidos**: Los problemas que existen en la compilación.
- **Puntos a tener en cuenta**: los aspectos importantes a tener en cuenta al usar la compilación.
- **Limitaciones**: Las limitaciones que existen en la compilación.

> **Importante:** Las notas de la versión de NetScaler Gateway se incluyen como parte de las notas de la versión de ADC.
> Para obtener información detallada sobre las mejoras de NetScaler Gateway 13.1, los problemas conocidos y las correcciones de errores, consulte la página de notas de la versión.

Nota:

- Las etiquetas [# XXXXXX] en las descripciones de los problemas son identificadores de seguimiento internos que utiliza el equipo de NetScaler.
- Estas notas de la versión no documentan las correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad.

Acerca de NetScaler Gateway

March 27, 2024

NetScaler Gateway es fácil de implementar y administrar. La configuración de implementación más típica consiste en localizar el dispositivo NetScaler Gateway en la DMZ. Puede instalar varios dispositivos NetScaler Gateway en la red para implementaciones más complejas.

La primera vez que inicie NetScaler Gateway, puede realizar la configuración inicial mediante una consola serie, el Asistente de configuración de la utilidad de configuración o el Protocolo de configuración dinámica de host (DHCP). En el dispositivo MPX, puede utilizar el teclado LCD del panel frontal del dispositivo para realizar la configuración inicial. Puede configurar ajustes básicos específicos de su red

interna, como la dirección IP, la máscara de subred, la dirección IP de la puerta de enlace predeterminada y la dirección del sistema de nombres de dominio (DNS). Después de configurar la configuración básica de la red, configure la configuración específica de la operación de NetScaler Gateway, como las opciones de autenticación, autorización, recursos de red, servidores virtuales, directivas de sesión y directivas de dispositivos de punto final.

Antes de instalar y configurar NetScaler Gateway, consulte los temas de esta sección para obtener información sobre cómo planificar la implementación. La planificación de la implementación puede incluir determinar dónde instalar el dispositivo, comprender cómo instalar varios dispositivos en la DMZ y los requisitos de licencia. Puede instalar NetScaler Gateway en cualquier infraestructura de red sin necesidad de realizar cambios en el hardware o software existente que se ejecuta en la red segura. NetScaler Gateway admite otros productos de red, como equilibradores de carga de servidores, motores de caché, firewalls, enrutadores y dispositivos inalámbricos IEEE 802.11.

Puede escribir la configuración en la lista de comprobación previa a la instalación para tenerlo a mano antes de configurar NetScaler Gateway.

Dispositivos NetScaler Gateway	Proporciona información sobre los dispositivos NetScaler Gateway y las instrucciones de instalación del dispositivo.
Lista de verificación de la instalación	Proporciona información de planificación para revisar y una lista de tareas que deben realizarse antes de instalar NetScaler Gateway en la red.
Implementaciones comunes	Proporciona información sobre la implementación de NetScaler Gateway en la DMZ de red, en una red segura sin DMZ y con otros dispositivos para admitir el equilibrio de carga y la conmutación por error. También proporciona información sobre la implementación de NetScaler Gateway con Citrix Virtual Apps and Desktops.
Licensing	Proporciona información sobre la instalación de licencias en el dispositivo. También proporciona información sobre la instalación de licencias en varios dispositivos NetScaler Gateway.

Arquitectura NetScaler Gateway

Los componentes principales de NetScaler Gateway son:

- **Servidores virtuales**. El servidor virtual de NetScaler Gateway es una entidad interna que representa todos los servicios configurados disponibles para los usuarios. El servidor virtual es también el punto de acceso a través del cual los usuarios acceden a estos servicios. Puede configurar varios servidores virtuales en un solo dispositivo, lo que permite que un dispositivo NetScaler Gateway atienda a varias comunidades de usuarios con distintos requisitos de autenticación y acceso a los recursos.
- **Autenticación, autorización y auditoría**. Puede configurar la autenticación, la autorización y la contabilidad para permitir a los usuarios iniciar sesión en NetScaler Gateway con credenciales que reconocen NetScaler Gateway o los servidores de autenticación ubicados en la red segura, como LDAP o RADIUS. Las directivas de autorización definen los permisos de usuario y determinan a qué recursos tiene autorización para acceder un usuario determinado. Para obtener más información sobre la autenticación y la autorización, consulte Configuración de la autenticación y la autorización. Los servidores de auditoría mantienen los datos sobre la actividad de NetScaler Gateway, incluidos los eventos de inicio de sesión de los usuarios, las instancias de acceso a los recursos y los errores operativos. Esta información se almacena en NetScaler Gateway o en un servidor externo. Para obtener más información sobre la auditoría, consulte Configuración de la auditoría en NetScaler Gateway.
- **Conexiones de usuarios**. Los usuarios pueden iniciar sesión en NetScaler Gateway mediante los siguientes métodos de acceso:
  - El cliente Citrix Secure Access para Windows es un software que se instala en un equipo basado en Windows. Los usuarios inician sesión haciendo clic con el botón derecho en un icono del área de notificación de un equipo basado en Windows. Si los usuarios utilizan un equipo en el que no está instalado el cliente Citrix Secure Access, pueden iniciar sesión mediante un explorador web para descargar e instalar el complemento. Si los usuarios tienen instalada la aplicación Citrix Workspace, inician sesión con el cliente Citrix Secure Access desde la aplicación Citrix Workspace. Cuando la aplicación Citrix Workspace y el cliente Citrix Secure Access están instalados en el dispositivo del usuario, la aplicación Citrix Workspace agrega el cliente Citrix Secure Access automáticamente.
  - El cliente Citrix Secure Access para macOS X que permite a los usuarios que ejecutan macOS X iniciar sesión. Tiene las mismas funciones y funciones que el cliente Citrix Secure Access para Windows. Puede proporcionar soporte de análisis de dispositivos de punto final para esta versión del complemento instalando NetScaler Gateway 10.1, compilación 120.1316.e.
  - Aplicación Citrix Workspace que permite conexiones de usuario a aplicaciones publicadas y escritorios virtuales de un conjunto de servidores mediante la Interfaz Web o Citrix StoreFront.
  - Aplicación Citrix Workspace, Secure Hub, WorxMail y WorxWeb que permiten a los usuarios

acceder a aplicaciones web y SaaS, aplicaciones móviles iOS y Android y datos de ShareFile alojados en Citrix Endpoint Management.

- Los usuarios pueden conectarse desde un dispositivo Android que utiliza la dirección web de NetScaler Gateway. Cuando los usuarios inician una aplicación, la conexión utiliza Micro VPN para dirigir el tráfico de red a la red interna. Si los usuarios se conectan desde un dispositivo Android, debe configurar la configuración de DNS en NetScaler Gateway. Para obtener más información, consulte Compatibilidad con consultas DNS mediante sufijos DNS para dispositivos Android.
- Los usuarios pueden conectarse desde un dispositivo iOS que utiliza la dirección web de NetScaler Gateway. Puede configurar Secure Browse de forma global o en un perfil de sesión. Cuando los usuarios inician una aplicación en su dispositivo iOS, se inicie una conexión VPN y la conexión se enruta a través de NetScaler Gateway.
- Acceso sin cliente que proporciona a los usuarios el acceso que necesitan sin instalar software en el dispositivo del usuario.

  Al configurar NetScaler Gateway, puede crear directivas para configurar cómo inician sesión los usuarios. También puede restringir el inicio de sesión de los usuarios mediante la creación de directivas de análisis de sesiones y endpoints.

- **Recursos de red**. Estos incluyen todos los servicios de red a los que los usuarios acceden a través de NetScaler Gateway, como servidores de archivos, aplicaciones y sitios web.
- **Adaptador virtual**. El adaptador virtual NetScaler Gateway admite aplicaciones que requieren suplantación de IP. El adaptador virtual se instala en el dispositivo del usuario cuando se instala el cliente Citrix Secure Access. Cuando los usuarios se conectan a la red interna, la conexión saliente entre NetScaler Gateway y los servidores internos usa la dirección IP de intranet como dirección IP de origen. El cliente Citrix Secure Access recibe esta dirección IP del servidor como parte de la configuración.

  Si habilita la tunelización dividida en NetScaler Gateway, todo el tráfico de la intranet se enruta a través del adaptador virtual. Al interceptar el tráfico vinculado a la intranet, el adaptador virtual interceptará consultas DNS de tipo de registro A y AAAA mientras deja intactas todas las demás consultas DNS. El tráfico de red que no está vinculado a la red interna se enruta a través del adaptador de red instalado en el dispositivo del usuario. Las conexiones a Internet y LAN privada (LAN) permanecen abiertas y conectadas. Si inhabilita la tunelización dividida, todas las conexiones se enrutan a través del adaptador virtual. Todas las conexiones existentes se desconectan y el usuario debe restablecer la sesión.

  Si configura una dirección IP de intranet, el tráfico hacia la red interna se falsificará con la dirección IP de la intranet a través del adaptador virtual.

Cómo funcionan las conexiones de usuario

Los usuarios pueden conectarse a sus correos electrónicos, recursos compartidos de archivos y otros recursos de red desde una ubicación remota. Los usuarios pueden conectarse a los recursos de la red interna con el siguiente software:

- Cliente Citrix Secure Access
- Aplicación Citrix Workspace
- WorxMail y WorxWeb
- Dispositivos móviles Android e iOS

Conéctese con el cliente Citrix Secure Access

El cliente Citrix Secure Access permite a los usuarios acceder a los recursos de la red interna mediante los siguientes pasos:

1. Un usuario se conecta a NetScaler Gateway por primera vez escribiendo la dirección web en un explorador web. Aparece la página de inicio de sesión y se solicita al usuario que introduzca un nombre de usuario y una contraseña. Si se configuran servidores de autenticación externos, NetScaler Gateway se pone en contacto con el servidor y los servidores de autenticación verifican las credenciales del usuario. Si se configura la autenticación local, NetScaler Gateway realiza la autenticación de usuarios.
2. Si configura una directiva de autenticación previa, cuando el usuario escribe la dirección web de NetScaler Gateway en un explorador web de un equipo basado en Windows o en un equipo macOS X, NetScaler Gateway comprueba si existen directivas de seguridad basadas en el cliente antes de que aparezca la página de inicio de sesión. Las comprobaciones de seguridad comprueban que el dispositivo del usuario cumple las condiciones relacionadas con la seguridad, como actualizaciones del sistema operativo, protección antivirus y un firewall configurado correctamente. Si el dispositivo del usuario no supera la comprobación de seguridad, NetScaler Gateway impide que el usuario inicie sesión. Un usuario que no puede iniciar sesión debe descargar las actualizaciones o los paquetes necesarios e instalarlos en el dispositivo del usuario. Cuando el dispositivo de usuario pasa la directiva de autenticación previa, aparece la página de inicio de sesión y el usuario puede introducir las credenciales de inicio de sesión. Puede usar Análisis avanzado de dispositivos de punto final en un equipo macOS X si instala NetScaler Gateway 10.1, compilación 120.1316.e.
3. Cuando NetScaler Gateway autentica correctamente al usuario, NetScaler Gateway inicie el túnel VPN. NetScaler Gateway solicita al usuario que descargue e instale el cliente Citrix Secure Access para Windows o el cliente Citrix Secure Access para macOS X.
4. Si configura un análisis posterior a la autenticación, después de que un usuario inicie sesión correctamente, NetScaler Gateway explora el dispositivo del usuario en busca de las directivas

de seguridad del cliente necesarias. Puede exigir las mismas condiciones relacionadas con la seguridad que para una directiva de autenticación previa. Si el dispositivo del usuario no supera el análisis, la directiva no se aplica o el usuario se coloca en un grupo de cuarentena y el acceso del usuario a los recursos de red es limitado.

5. Cuando se establece la sesión, se dirige al usuario a una página principal de NetScaler Gateway, donde el usuario puede seleccionar los recursos a los que acceder. La página principal incluida en NetScaler Gateway se denomina Interfaz de acceso. Si el usuario inicie sesión mediante el cliente Citrix Secure Access para Windows, aparecerá un icono en el área de notificación del escritorio de Windows que indica que el dispositivo del usuario está conectado y el usuario recibe un mensaje en el que se indica que la conexión se ha establecido. El usuario también puede acceder a los recursos de la red sin utilizar la interfaz de acceso, como abrir Microsoft Outlook y recuperar correo electrónico.
6. Si la solicitud de usuario pasa las comprobaciones de seguridad previas y versiones posteriores a la autenticación, NetScaler Gateway se pone en contacto con el recurso solicitado e inicie una conexión segura entre el dispositivo de usuario y ese recurso.
7. El usuario puede cerrar una sesión activa haciendo clic con el botón secundario en el icono de NetScaler Gateway del área de notificación de un equipo basado en Windows y, a continuación, haciendo clic en Cerrar sesión. La sesión también puede agotarse debido a la inactividad. Cuando se cierra la sesión, el túnel se cierra y el usuario ya no tiene acceso a los recursos internos. El usuario también puede escribir la dirección web de NetScaler Gateway en un explorador. Cuando el usuario presiona Intro, aparece la interfaz de acceso desde la que los usuarios pueden cerrar la sesión.

Nota: Si implementa Citrix Endpoint Management en su red interna, un usuario que se conecte desde fuera de la red interna debe conectarse primero a NetScaler Gateway. Cuando el usuario establece la conexión, el usuario puede acceder a aplicaciones web y SaaS, aplicaciones móviles Android e iOS y datos de ShareFile alojados en Citrix Endpoint Management. Un usuario puede conectarse con el cliente Citrix Secure Access mediante el acceso sin cliente o mediante la aplicación Citrix Workspace o Secure Hub.

Conéctese con la aplicación Citrix Workspace

Los usuarios pueden conectarse con la aplicación Citrix Workspace para acceder a sus aplicaciones y escritorios virtuales basados en Windows. Los usuarios también pueden acceder a las aplicaciones desde Endpoint Management. Para conectarse desde una ubicación remota, los usuarios también instalan el cliente Citrix Secure Access en su dispositivo. La aplicación Citrix Workspace agrega automáticamente el cliente Citrix Secure Access a su lista de complementos. Cuando los usuarios inician sesión en la aplicación Citrix Workspace, también pueden iniciar sesión en el cliente Citrix Secure Access. También puede configurar NetScaler Gateway para que realice un inicio de sesión único en el cliente Citrix Secure Access cuando los usuarios inicien sesión en la aplicación Citrix Workspace.

Conéctate con dispositivos iOS y Android

Los usuarios pueden conectarse desde un dispositivo iOS o Android mediante Secure Hub. Los usuarios pueden acceder a su correo electrónico mediante Secure Mail y conectarse a sitios web con WorxWeb.

Cuando los usuarios se conectan desde el dispositivo móvil, las conexiones se dirigen a través de NetScaler Gateway para acceder a los recursos internos. Si los usuarios se conectan con iOS, habilita Secure Browse como parte del perfil de sesión. Si los usuarios se conectan con Android, la conexión utiliza la Micro VPN automáticamente. Además,
Secure Mail y WorxWeb utilizan Micro VPN para establecer conexiones a través de NetScaler Gateway. No es necesario configurar Micro VPN en NetScaler Gateway.

Implementaciones comunes de NetScaler Gateway

January 26, 2024

Es posible implementar NetScaler Gateway en el perímetro de la red interna (o intranet) de la organización para proporcionar un único punto de acceso seguro a los servidores, las aplicaciones y otros recursos de red que residan en la red interna. Todos los usuarios remotos deben conectarse a NetScaler Gateway para poder acceder a los recursos de la red interna.

NetScaler Gateway suele instalarse en las siguientes ubicaciones de una red:

- En la red DMZ
- En una red segura que no tiene una DMZ

También puede implementar NetScaler Gateway con Citrix Virtual Apps, Citrix Virtual Desktops, StoreFront y Citrix Endpoint Management para permitir a los usuarios acceder a sus aplicaciones Windows, web, móviles y SaaS. Si su implementación incluye Citrix Virtual Apps, StoreFront y Desktops 7, puede implementar NetScaler Gateway en una configuración DMZ de salto único o doble salto. Las implementaciones de doble salto no son compatibles con versiones anteriores de Citrix Virtual Desktops ni Citrix Endpoint Management.

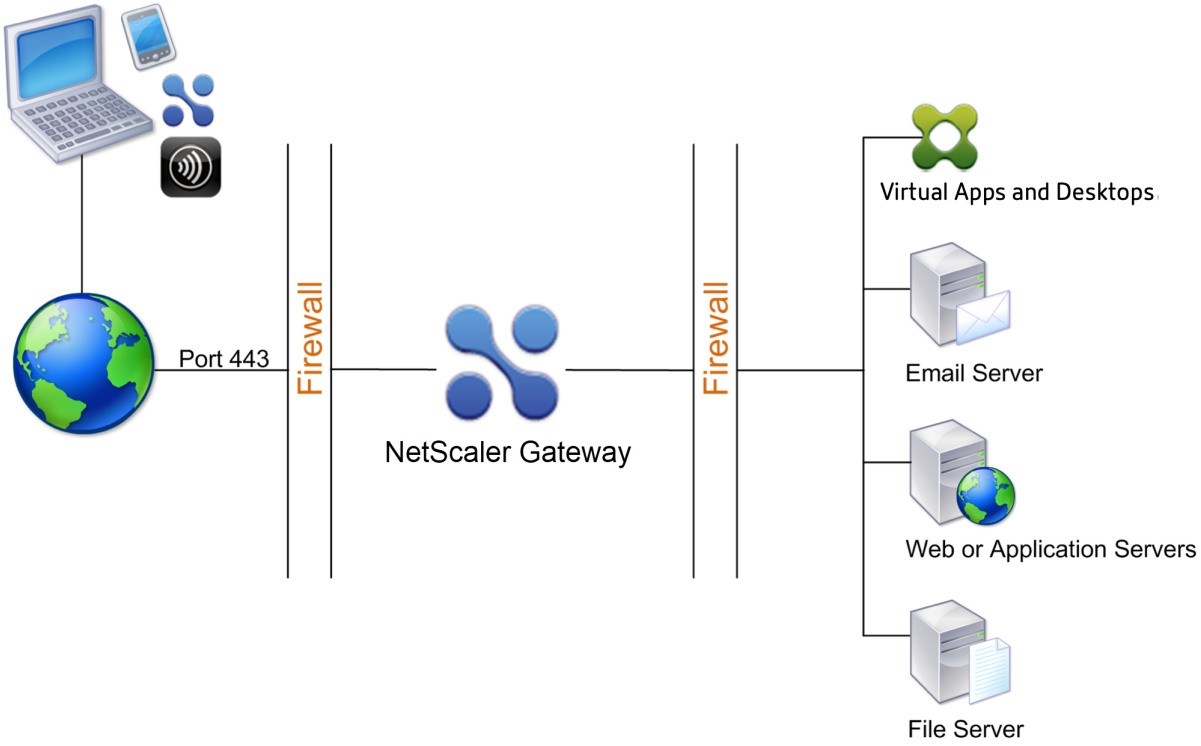
Para obtener más información sobre cómo ampliar la instalación de NetScaler Gateway con estas y otras soluciones de NetScaler compatibles, consulte el tema Integración con los productos de NetScaler.

Implementación de NetScaler Gateway en una DMZ

Muchas organizaciones protegen su red interna con una DMZ. Una DMZ es una subred que se encuentra entre la red interna segura de una organización e Internet (o cualquier red externa). Al implemen-

tar NetScaler Gateway en la DMZ, los usuarios se conectan con la aplicación Citrix Secure Access para Windows o Citrix Workspace.

Figura 1. NetScaler Gateway implementado en la DMZ



En la configuración que se muestra en la ilustración anterior, se instala NetScaler Gateway en la DMZ y se configura para que se conecte tanto a Internet como a la red interna.

Conectividad de NetScaler Gateway en una DMZ

Al implementar NetScaler Gateway en la DMZ, las conexiones de usuario deben atravesar el primer firewall para conectarse a NetScaler Gateway. De forma predeterminada, las conexiones de usuario utilizan SSL en el puerto 443 para establecer esta conexión. Para permitir que las conexiones de usuario lleguen a la red interna, debe permitir SSL en el puerto 443 a través del primer firewall.

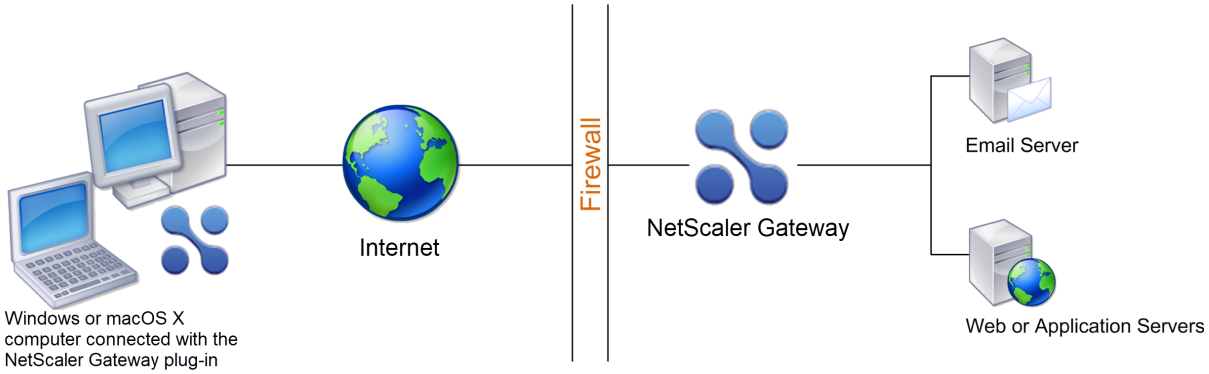
NetScaler Gateway descifra las conexiones SSL del dispositivo del usuario y establece una conexión en nombre del usuario con los recursos de red detrás del segundo firewall. Los puertos que deben abrirse a través del segundo firewall dependen de los recursos de red a los que autoriza el acceso de los usuarios externos.

Por ejemplo, si autoriza a los usuarios externos a acceder a un servidor web de la red interna y este servidor escucha conexiones HTTP en el puerto 80, debe permitir HTTP en el puerto 80 a través del segundo firewall. NetScaler Gateway establece la conexión a través del segundo firewall con el servidor HTTP de la red interna en nombre de los dispositivos de usuario externos.

Implementación de NetScaler Gateway en una red segura

Puede instalar NetScaler Gateway en la red segura. En este caso, un firewall se interpone entre Internet y la red segura. NetScaler Gateway reside en el firewall para controlar el acceso a los recursos de la red.

Figura 1. NetScaler Gateway implementado en la red segura



Al implementar NetScaler Gateway en la red segura, conecte una interfaz de NetScaler Gateway a Internet y la otra interfaz a los servidores que se ejecutan en la red segura. La colocación de NetScaler Gateway en la red segura proporciona acceso a los usuarios locales y remotos. Debido a que esta configuración solo tiene un firewall, hace que la implementación sea menos segura para los usuarios que se conectan desde una ubicación remota. Aunque NetScaler Gateway intercepta el tráfico de Internet, el tráfico entra en la red segura antes de que los usuarios se autentiquen. Cuando NetScaler Gateway se implementa en una DMZ, los usuarios se autentican antes de que el tráfico de red llegue a la red segura.

Cuando NetScaler Gateway se implementa en la red segura, las conexiones de Citrix Secure Access para Windows deben atravesar el firewall para conectarse a NetScaler Gateway. De forma predeterminada, las conexiones de usuario utilizan el protocolo SSL del puerto 443 para establecer esta conexión. Para admitir esta conectividad, debe abrir el puerto 443 en el firewall.

Requisitos de software cliente

March 27, 2024

NetScaler Gateway admite conexiones de usuario mediante el cliente Citrix Secure Access. Cuando los usuarios inician sesión con el complemento, se establece un túnel VPN completo. Con el cliente Citrix Secure Access, los usuarios pueden conectarse a los recursos de red a los que usted permite el acceso.

Si las directivas de punto final están configuradas en NetScaler Gateway, NetScaler Gateway descarga e instala el cliente Citrix EPA en el dispositivo del usuario automáticamente cuando los usuarios inician sesión.

Requisitos del sistema cliente Citrix Secure Access

El cliente Citrix Secure Access establece una conexión segura desde el equipo cliente al dispositivo NetScaler Gateway.

El complemento se distribuye como aplicación de escritorio para los sistemas operativos Microsoft Windows, macOS X y Linux. Después de autenticarse en la URL segura del dispositivo NetScaler Gateway con el explorador web, el complemento se descarga e instala automáticamente en el equipo.

El plug-in se aprovisiona como aplicación móvil para dispositivos Android e iOS.

> **Nota:**
>
> - Para instalar el plug-in, se necesitan privilegios de administrador y root en el sistema operativo.
> - Los exploradores web que admiten el cliente Citrix Secure Access también admiten la VPN sin cliente.

El cliente Citrix Secure Access como aplicación de escritorio es compatible con los siguientes sistemas operativos y exploradores web.

Sistema operativo	Exploradores Web compatibles
macOS X (10.9 y posteriores)	Safari 7.1 o posterior; Google Chrome versión 30 o posterior; Mozilla Firefox versión 30 o posterior
Windows 11	Versión 30 de Google Chrome o una posterior; versión 24 de Mozilla Firefox o una posterior; Edge Chromium
Windows 10 (x86 y x64)	Versión 30 de Google Chrome o una posterior; versión 24 de Mozilla Firefox o una posterior; Edge Chromium
Linux; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.	Mozilla Firefox versión 44 y superior; Google Chrome 50 y superior

> **Nota:**

> Actualmente, el cliente Citrix Secure Access y el cliente Citrix EPA para Ubuntu solo admiten el administrador de pantalla predeterminado de GNOME.

Si faltan los paquetes de dependencias necesarios, el comando los enumera y se produce un error en la instalación del complemento. Estos paquetes de dependencias se deben instalar manualmente. Los administradores pueden instalar un paquete que falta escribiendo el siguiente comando mediante la interfaz de línea de comandos.

```
apt-get install <dependency package>
<!--NeedCopy-->
```

El cliente Citrix Secure Access como aplicación móvil es compatible con los siguientes sistemas operativos.

Aplicación VPN	Sistemas operativos compatibles
Android	Android 7.0 y versiones posteriores
iOS	iOS 12.0 y versiones posteriores

> **Nota:**
>
> Si utiliza las versiones más recientes de Apple OS, como macOS 14/iOS 17 y versiones posteriores, le recomendamos que actualice al cliente Citrix Secure Access o a la versión 23.09.1 de Citrix SSO o posterior.

requisitos de Endpoint Analysis

NetScaler Gateway instala el cliente Citrix EPA en el dispositivo del usuario. El cliente Citrix EPA analiza el dispositivo del usuario en busca de los requisitos de seguridad de los endpoints que ha configurado en NetScaler Gateway. Los requisitos incluyen información, como el sistema operativo, el antivirus o las versiones del explorador web.

Cuando los usuarios se conectan a NetScaler Gateway mediante el explorador por primera vez, el portal solicita la instalación del cliente Citrix EPA. En los siguientes intentos de inicio de sesión, el cliente Citrix EPA verifica la configuración del control de actualizaciones para confirmar si es necesaria la actualización del cliente Citrix EPA. Si es necesario, el usuario recibe un mensaje para descargar e instalar el cliente Citrix EPA más reciente. El cliente Citrix EPA para Windows se instala como una aplicación Windows de 32 bits. El cliente Citrix EPA para macOS se instala como una aplicación de 64 bits. No se requieren privilegios especiales para instalar o usar el cliente Citrix EPA, excepto cuando se usa EPA para acceder a los certificados de los dispositivos. Para obtener más información sobre cómo usar la EPA para la autenticación de certificados de dispositivos, consulte Usar certificados de dispositivos para la autenticación.

La información sobre herramientas de la consola de la interfaz de usuario de administración explica los análisis en detalle. Para obtener más información sobre las bibliotecas de EPA, consulte https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/.

> **Importante:**
>
> - Los exploradores compatibles con EPA también admiten VPN sin cliente.
> - En el análisis de puntos finales previo a la autenticación, el usuario no puede iniciar sesión en el cliente Citrix Secure Access si no instala el complemento Endpoint Analysis o se salta el escaneo.
> - En el análisis de endpoint posterior a la autenticación, el usuario puede acceder a los recursos para los que no es necesario realizar un análisis mediante el acceso sin cliente o mediante la aplicación Citrix Workspace.
> - Para los análisis relacionados con OPSWAT, debe instalar el paquete binario `epaPackage.exe` en el equipo cliente.

Se necesita el siguiente software en los dispositivos de usuario para utilizar el complemento Endpoint Analysis:

Sistema operativo	Exploradores Web compatibles
macOS (10.9 y posteriores)	Safari 7.1 o posterior; Google Chrome versión 30 o posterior; Mozilla Firefox versión 30 o posterior
Windows 11	Versión 30 de Google Chrome o una posterior; versión 24 de Mozilla Firefox o una posterior; Edge Chromium
Windows 10	Versión 30 de Google Chrome o una posterior; versión 24 de Mozilla Firefox o una posterior; Edge Chromium
Linux; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.	Mozilla Firefox versión 44 y posteriores; Google Chrome 50 y versiones posteriores

Nota:

- Todas las ediciones de las variantes del sistema operativo mencionadas anteriormente son compatibles.
- No se admiten Windows 10 y Windows 11 en los modos S.
- Para las ediciones de Windows, se deben instalar todos los service packs y las actualizaciones críticas.

- Para las versiones de Mozilla Firefox, el análisis de puntos finales debe estar habilitado para el complemento. La versión mínima requerida es 3.0.

Compatibilidad de NetScaler Gateway con los productos NetScaler

March 27, 2024

La siguiente tabla proporciona los productos y las versiones de NetScaler con los que NetScaler Gateway 13.1 es compatible.

> **Nota:**
>
> Las funciones de NetScaler Gateway están disponibles en NetScaler VPX.

Productos y versiones compatibles de NetScaler

Producto NetScaler	Versión de lanzamiento
Citrix SD-WAN	10.2, 11.0
Plataformas NetScaler	Todos los modelos MPX y VPX actuales, incluidos los dispositivos compatibles con FIPS.
StoreFront	Todas las versiones de StoreFront compatibles actualmente.
Citrix Virtual Apps and Desktops	7.15, 1808, 1811, 1903, 1906, 1909, 2003, 2009, 2112, 1912 LTSR, 2203 LTSR
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

Aplicaciones Citrix Workspace, aplicaciones móviles de productividad de Citrix y complementos

*La primera compilación compatible para cada versión de software se indica en la tabla siguiente.Se admiten todas las compilaciones posteriores, a menos que se especifique lo contrario. Para obtener más información sobre el ciclo de vida de las versiones, consulte lamatriz de productos.

Aplicación o complemento Citrix Workspace	Versión mínima compatible*
Cliente Citrix Secure Access para macOS X	3.1.8

Aplicación o complemento Citrix Workspace	Versión mínima compatible*
Cliente Citrix Secure Access para Windows	12.0
Cliente Citrix Secure Access para iOS	3.1.4
Cliente Citrix Secure Access para Android	2.0.14
Aplicación Citrix Workspace para Android	3.11
Aplicación Citrix Workspace para iOS	7.1.3
Aplicación Citrix Workspace para Mac	12.4
Aplicación Citrix Workspace para Windows	4.4
Aplicación Citrix Workspace para Linux	13.4
Aplicación Citrix Workspace para HTML5	2.3
Aplicación Citrix Workspace para Chrome	2.3
Secure Hub para iOS	10.5
Secure Hub para Android	10.5
Secure Mail para iOS	10.5
SecureWeb para iOS	10.5
Secure Mail para Android	10.5
SecureWeb para Android	10.5

> **Nota:**
>
> - Para obtener información detallada sobre algunas de las funciones de uso común compatibles con cada cliente VPN, consulte Clientes VPN de NetScaler Gateway y funciones compatibles.

Licencias de NetScaler Gateway

January 26, 2024

Después de instalar NetScaler Gateway, puede obtener los archivos de licencia Platform o Universal de Citrix. Inicie sesión en el sitio web de Citrix para acceder a las licencias disponibles y generar un archivo de licencia. Una vez generado el archivo de licencia, lo descarga en un equipo. Cuando el

archivo de licencia está en el equipo, lo carga en NetScaler Gateway. Para obtener más información sobre las licencias de Citrix, consulte Citrix Licensing System.

Antes de obtener los archivos de licencia, asegúrese de configurar el nombre de host del dispositivo mediante el Asistente de configuración y, a continuación, reinicie el dispositivo.

Para obtener sus licencias, vaya a la página web Activar, actualizar y administrar licencias de NetScaler. En esta página, puede obtener su nueva licencia y activar, actualizar y administrar las licencias de NetScaler.

Importante:

> - Debe instalar licencias en NetScaler Gateway. El dispositivo no obtiene licencias del servidor de licencias de NetScaler.
> - Citrix recomienda conservar una copia local de todos los archivos de licencia que reciba. Al guardar una copia de seguridad del archivo de configuración, todos los archivos de licencia cargados se incluyen en la copia de seguridad. Si debe volver a instalar el software del dispositivo NetScaler Gateway y no tiene una copia de seguridad de la configuración, necesitará los archivos de licencia originales.

Antes de instalar licencias en NetScaler Gateway, establezca el nombre de host del dispositivo y, a continuación, reinicie NetScaler Gateway. Utilice el Asistente de configuración para configurar el nombre de host. Al generar la licencia universal para NetScaler Gateway, el nombre de host se utiliza en la licencia.

Tipos de licencia de NetScaler Gateway

NetScaler Gateway requiere una licencia de plataforma. La licencia de plataforma permite un número ilimitado de conexiones a Citrix Virtual Apps, Citrix Virtual Desktops o StoreFront mediante ICA Proxy. Para permitir las conexiones VPN a la red desde el cliente Citrix Secure Access, un punto de inicio de sesión de SmartAccess o Secure Hub, WorxWeb o Secure Mail, también debe agregar una licencia universal. NetScaler Gateway VPX incluye la licencia Platform.

La licencia de plataforma es compatible con las siguientes versiones de NetScaler Gateway:

- NetScaler Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- NetScaler VPX

> **Importante:** Citrix recomienda conservar una copia local de todos los archivos de licencia que reciba. Al guardar una copia de seguridad del archivo de configuración, todos los archivos de licencia cargados se incluyen en la copia de seguridad. Si necesita volver a instalar el software del dispositivo NetScaler Gateway y no tiene una copia de seguridad de la configuración, necesitará los archivos de licencia originales.

La licencia de plataforma

La licencia Platform permite conexiones ilimitadas de usuarios a aplicaciones publicadas en Citrix Virtual Apps o escritorios virtuales de Citrix Virtual Desktops. Las conexiones mediante Citrix Receiver no utilizan una licencia universal de NetScaler Gateway. Estas conexiones solo necesitan la licencia Platform. La licencia de plataforma se entrega electrónicamente con todos los pedidos nuevos de NetScaler Gateway, ya sean físicos o virtuales. Si ya posee un dispositivo cubierto por una garantía o un acuerdo de mantenimiento, puede obtener la licencia de plataforma en el sitio web de Citrix.

La licencia universal

La licencia universal de NetScaler Gateway limita el número de sesiones de usuario simultáneas al número de licencias adquiridas. Si compra 100 licencias, puede tener 100 sesiones simultáneas en cualquier momento. Si adquiere una licencia de modificación estándar, puede tener 500 sesiones simultáneas en cualquier momento. Cuando un usuario finaliza una sesión, esa licencia se libera para el siguiente usuario. Un usuario que inicia sesión en NetScaler Gateway desde más de un equipo ocupa una licencia para cada sesión.

Si todas las licencias están ocupadas, no se pueden abrir conexiones adicionales hasta que un usuario finaliza una sesión o el administrador finaliza la sesión mediante la utilidad de configuración. Cuando se cierra una conexión, la licencia se libera y se puede utilizar para un nuevo usuario.

Cuando recibe el dispositivo NetScaler Gateway, la licencia se realiza en el siguiente orden:

- Recibirá el código de acceso a la licencia (clave de licencia) en un correo electrónico.
- Utilice el Asistente de configuración para configurar NetScaler Gateway con el nombre de host.
- Las licencias de NetScaler Gateway se asignan desde el sitio web de Citrix. Utilice el nombre de host para enlazar las licencias al dispositivo durante el proceso de asignación.
- Instale el archivo de licencia en NetScaler Gateway.

La licencia Universal admite las siguientes funciones:

- Túnel VPN completo
- Micro VPN
- Análisis de dispositivos de punto final

- SmartAccess basado en directivas
- Acceso sin cliente a sitios web y recursos compartidos de archivos

Obtención de la licencia universal Necesita la siguiente información antes de ir al sitio web de Citrix para obtener la licencia universal.

- El ID de usuario y la contraseña de su cuenta Citrix.

  Regístrese en el sitio web de Citrix (https://www.citrix.com/welcome/create-account/) para recibir su ID de usuario y contraseña.
  Nota: Si no encuentra el código de licencia ni el ID de usuario y la contraseña, póngase en contacto con el servicio de atención al cliente de Citrix.

- El nombre de host de
  NetScaler Gateway

  El campo de entrada de este nombre en el sitio web de Citrix distingue entre mayúsculas y minúsculas, así que asegúrese de copiar el nombre de host exactamente como está configurado en el dispositivo NetScaler.

- Número de licencias que quiere incluir en el archivo de licencia

  No es necesario descargar todas las licencias a las que se tiene derecho de una sola vez. Por ejemplo, si su empresa ha adquirido 100 licencias, puede elegir descargar 50. Puede asignar el resto en otro archivo de licencia más adelante. Se pueden instalar varios archivos de licencia en
  NetScaler Gateway.

  Nota: Antes de obtener las licencias, asegúrese de configurar el nombre de host del dispositivo NetScaler mediante el asistente de configuración y, a continuación, reinicie el dispositivo.

Para obtener la licencia universal

1. Inicie sesión en el sitio web de Citrix (https://www.citrix.com/en-in/account/) con sus credenciales de Citrix.
2. En **Citrix Manage Licenses está aquí**, siga las instrucciones para obtener su archivo de licencia.

Instalación de la licencia universal Para instalar la licencia, consulte "Instalación de la licencia". Después de la instalación, compruebe que la licencia se instaló correctamente.

Verificar la instalación de la licencia universal Antes de continuar, compruebe que la licencia universal está instalada correctamente.

Para verificar la instalación de la licencia universal mediante la CLI

1. Abra una conexión SSH con el dispositivo NetScaler mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo NetScaler con las credenciales de administrador.
3. Utilice el comando show license para verificar que "SSL VPN = SÍ"y que el número máximo de usuarios ha aumentado de 5 al número esperado de usuarios simultáneos.

Para verificar la instalación de la licencia universal mediante la interfaz gráfica de usuario

1. En un explorador web, escriba la dirección IP del dispositivo NetScaler, como `http://192.168.100.1`.
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. En el panel de navegación, expanda Sistemay, a continuación, haga clic en Licencias.
4. En el panel Licencias, aparece una marca de verificación verde junto a **NetScaler Gateway**. El campo Máximo de usuarios de NetScaler Gateway permitidos muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo NetScaler.

Recursos conexos

- Sistema de licencias Citrix
- Hoja de datos de NetScaler
- Tipos de licencias de NetScaler y NetScaler Gateway

Instalar una licencia en NetScaler Gateway

March 27, 2024

Después de descargar correctamente el archivo de licencia en su equipo, podrá instalar la licencia en NetScaler Gateway. La licencia se instala en el directorio /nsconfig/licence/.

Si utilizó el Asistente de configuración para configurar la configuración inicial de NetScaler Gateway, el archivo de licencia se instala al ejecutar el asistente. Si asigna parte de las licencias y, posteriormente, asigna un número adicional, puede instalar las licencias sin utilizar el Asistente de configuración.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Licencias** .
2. En el panel de detalles, haga clic en **Administrar licencias**.
3. Haga clic en **Agregar nueva licencia**, luego en **Examinar**, vaya a el archivo de licencia y, a continuación, haga clic en **Aceptar**.

Aparece un mensaje en la utilidad de configuración que indica que debe reiniciar NetScaler Gateway. Haga clic en Reiniciar.

Establecer el número máximo de usuarios

Después de instalar la licencia en el dispositivo, debe establecer el número máximo de usuarios que pueden conectarse al dispositivo. Establezca el máximo de usuarios en la directiva de autenticación global.

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway**y, a continuación, haga clic en Configuración global.**
2. En el panel de detalles, en Configuración, haga clic en **Cambiar la configuración de autenticación AAA**.
3. En Número máximo de usuarios, escriba el número total de usuarios y, a continuación, haga clic en **Aceptar**.

   El número de este campo corresponde a la cantidad de licencias que contiene el archivo de licencias. Este número debe ser inferior o igual al número total de licencias instaladas en el dispositivo. Por ejemplo, instale una licencia que contenga 100 licencias de usuario y otra que contenga 400 licencias de usuario. El total de licencias es igual a 500. El máximo de usuarios que pueden iniciar sesión es igual o inferior a 500. Si 500 usuarios han iniciado sesión, a todos los usuarios que intenten iniciar sesión más allá de ese número se les deniega el acceso hasta que un usuario cierra la sesión o finaliza una sesión.

Verificar la instalación de la licencia universal

Antes de continuar, compruebe que la licencia Universal está instalada correctamente.

Para verificar la instalación de la licencia universal mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Licencias .

   En el panel Licencias, aparece una marca de verificación verde junto a NetScaler Gateway. El campo Número máximo de usuarios de NetScaler Gateway permitidos muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo.

Para comprobar la instalación de la licencia universal mediante la CLI

1. Abra una conexión de Secure Shell (SSH) con el dispositivo mediante un cliente SSH, como PuTTY.
2. Inicie sesión en el dispositivo con las credenciales de administrador.
3. En el símbolo del sistema, escriba;

```
show license
<!--NeedCopy-->
```

La licencia se instala correctamente si el parámetro SSL VPN es igual a Sí y el parámetro de usuarios máximos es igual al número de licencias.

Preguntas frecuentes sobre licencias de NetScaler Gateway

January 26, 2024

¿Cómo puedo obtener ayuda con las licencias de prueba o demo?

Muchos de los productos de NetScaler ahora se ofrecen como experiencias de demostración completas, privadas y 1:1 dirigidas por expertos. Nuestros expertos de Citrix personalizan la demostración para adaptarla a sus necesidades, casos de uso y proyectos activos. No se requieren descargas, licencias ni instalación. Necesitas una configuración mínima para ver una demostración instantánea. Después de la demostración, para proceder con una prueba de concepto o prueba de una solución Citrix aplicable a sus servicios, póngase en contacto con los expertos de Citrix. Para ver demostraciones, haga clic en https://demo.citrix.com/.

¿Cómo instalar licencias?

Para obtener más información sobre la instalación de licencias, consulte Para instalar una licencia en NetScaler Gateway.

¿Cuáles son los distintos tipos de licencias de Gateway?

La licencia de plataforma permite un número ilimitado de conexiones a Citrix Virtual Apps, Citrix Virtual Desktops o StoreFront mediante ICA Proxy.
La licencia universal es una licencia complementaria a las licencias de la plataforma NetScaler. Esto

permite las conexiones VPN a la red desde el cliente Citrix Secure Access, un punto de inicio de sesión de SmartAccess o Secure Hub, Secure Web o Secure Mail. Para obtener más información, consulte Tipos de licencia de NetScaler Gateway.

¿Cuántas sesiones de usuario simultáneas se admiten?

Las sesiones admitidas dependen del tipo de licencia de puerta de enlace. Para obtener más información, consulte Tipos de licencia de NetScaler Gateway.

Otro factor a tener en cuenta es la capacidad del propio hardware subyacente. Consulte la hoja de datos de NetScaler MPX/SDX o la hoja de datos de NetScaler VPX para obtener información sobre el rendimiento.

¿Cómo comprobar las sesiones de usuario simultáneas actuales con licencia?

En la utilidad de configuración de la ficha Configuración, expanda **Sistema** y, a continuación, haga clic en **Licencias**.
En el panel **Licencias**, aparece una marca de verificación verde junto a NetScaler Gateway. El campo Número **máximo de usuarios de NetScaler Gateway permitidos** muestra el número de sesiones de usuario simultáneas con licencia en el dispositivo.

¿Cómo comprobar si se alcanza el límite de rendimiento de la licencia?

Puede extraer el rendimiento en tiempo real mediante `newnslog`. Por ejemplo, si el rendimiento de la licencia es de 500 Mbps, puede extraer el rendimiento en tiempo real superior a 500 mediante el siguiente comando.

```
nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index  rtime totalcount-val     delta rate/sec symbol-name&device-no&time
    12   7000      801130681      3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13      0      460776045      3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14   7000      801134437      3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15      0      460779784      3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16   7000      801138166      3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17      0      460783497      3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18   7000      801141896      3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19      0      460787213      3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20   7000      801145623      3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21      0      460790929      3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22   7000      801149353      3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23      0      460794646      3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24   7000      801153067      3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25      0      460798342      3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```


¿Cómo comprobar si los paquetes se pierden al alcanzar el rendimiento de las licencias?

Puede utilizar el siguiente comando para comprobar si se descartan paquetes.

```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index    rtime    totalcount-val      delta rate/sec symbol-name&device-no&time
     0 1966993          23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
     1       0          48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
     2       0        8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
     3    7000          23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
     4       0          48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
     5       0        8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
     6    7000          23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
     7       0          48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
     8       0        8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

¿Cómo puedo averiguar cuál es el rendimiento con licencia de un dispositivo NetScaler?

Ejecute el comando `show license` desde la CLI y, a continuación, utilice el número de modelo para obtener el rendimiento de la hoja de datos de MPX, SDX y VPX de ADC o gateway.


```
> sh license
       License status:
                          Web Logging: YES
                     Surge Protection: YES
                       Load Balancing: YES
                    Content Switching: YES
                    Cache Redirection: YES
                         Sure Connect: YES
                  Compression Control: YES
                    Delta Compression: NO
                     Priority Queuing: YES
                       SSL Offloading: YES
          Global Server Load Balancing: YES
                       GSLB Proximity: YES
                  Http DoS Protection: YES
                      Dynamic Routing: YES
                    Content Filtering: YES
                   Integrated Caching: YES
                              SSL VPN: YES   (Maximum users = 5)   (Maximum ICA u
sers = 0)
                                  AAA: YES
                          OSPF Routing: YES
                           RIP Routing: YES
                           BGP Routing: YES
                              Rewrite: YES
              IPv6 protocol translation: YES
                   Application Firewall: YES
                             Responder: YES
                        HTML Injection: YES
                        NetScaler Push: YES
                  Web Interface on NS: YES
                              AppFlow: YES
                          CloudBridge: YES
                     Model Number ID: 5500
 Done
> 
```

CITRIX

Citrix NetScaler | Datasheet

NetScaler platform	MPX 9500	MPX 7500	MPX 5500	VPX 10/200/1000/3000
Platform attributes				
Processor	Intel Xeon L5410 (4 cores total)	Intel Xeon L5410 (4 cores total)	Intel Xeon E5205 (2 cores total)	Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™
Memory	8 GB	8 GB	4 GB	
Ethernet ports	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	4x 10/100/1000 BASE-T	• Citrix® XenServer® 5 (update 3 or better) • Windows Server 2008 R2 with Hyper-V role • VMWare ESX/ESXi 3.5 or higher • 4G RAM/20 GB hard drive • Hypervisor supported NIC
Transceivers support	SX, LX	SX, LX		
Software upgradable performance		Upgrade option to MPX 9500		Upgrade options to VPX 200, VPX 1000 and VPX 3000
Platform performance				
System throughput, Gbps	3	1	0.5	Up to 3.0[2]
HTTP requests/sec	200,000	100,000	50,000	Up to 100,000
SSL transactions/sec	20,000	10,000	5,000	Up to 500
SSL throughput, Gbps	3	1	0.5	Up to 1.0
Compression throughput, Gbps	2	1	0.5	Up to 0.75
SSL VPN: concurrent users	10,000	10,000	5,000	Up to 300[3]

¿Cómo agregar más usuarios a las licencias de Gateway existentes?

Puede instalar una licencia universal adicional. Por ejemplo, supongamos que ha instalado una licencia universal que contiene 100 licencias de usuario. Si instala la segunda licencia universal que contiene 400 licencias de usuario, el número total de licencias de usuario es igual a 500.

Antes de empezar

March 27, 2024

Antes de instalar NetScaler Gateway, debe evaluar su infraestructura y recopilar información para planificar una estrategia de acceso que satisfaga las necesidades específicas de su organización. Al definir su estrategia de acceso, debe tener en cuenta las implicaciones de seguridad y completar un análisis de riesgos. También debe determinar las redes a las que los usuarios pueden conectarse y decidir las directivas que permiten las conexiones de los usuarios.

Además de planificar los recursos disponibles para los usuarios, también debe planificar el caso de implementación. NetScaler Gateway es compatible con los siguientes productos de NetScaler:

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Interfaz Web
- Citrix SD-WAN

Para obtener más información sobre la implementación de NetScaler Gateway, consulte [Implementaciones comunes](/es-es/netscaler-gateway/current-release/common-deployments.html)e integración con productos de NetScaler

Al preparar la estrategia de acceso, realice los siguientes pasos preliminares:

- Identificar recursos. Enumere los recursos de red a los que quiere proporcionar acceso, como aplicaciones web, SaaS, móviles o publicadas, escritorios virtuales, servicios y datos que ha definido en el análisis de riesgos.
- Desarrolle casos de acceso. Cree casos de acceso que describan cómo los usuarios acceden a los recursos de la red. Un caso de acceso lo define el servidor virtual utilizado para acceder a la red, los resultados del análisis de puntos finales, el tipo de autenticación o una combinación de los mismos. También puede definir cómo los usuarios inician sesión en la red.
- Identificar el software cliente. Puede proporcionar acceso completo a la VPN con el cliente Citrix Secure Access, exigiendo a los usuarios que inicien sesión con la aplicación Citrix Workspace,

Secure Hub o mediante el acceso sin cliente. También puede restringir el acceso al correo electrónico a Outlook Web App o WorxMail. Estos casos de acceso también determinan las acciones que los usuarios pueden realizar cuando obtienen acceso. Por ejemplo, puede especificar si los usuarios pueden modificar documentos mediante una aplicación publicada o conectándose a un recurso compartido de archivos.

- Asocie directivas a usuarios, grupos o servidores virtuales. Las directivas que crea en NetScaler Gateway se aplican cuando la persona o el conjunto de usuarios cumplen las condiciones especificadas. Las condiciones se determinan en función de los casos de acceso que cree. A continuación, crea directivas que amplían la seguridad de la red mediante el control de los recursos a los que pueden acceder los usuarios y las acciones que los usuarios pueden realizar en esos recursos. Las directivas se asocian a los usuarios, grupos, servidores virtuales adecuados o de forma global.

En esta sección se incluyen los siguientes temas para ayudarle a planificar su estrategia de acceso:

- Planning for Security incluye información sobre autenticación y certificados.
- Requisitos previos que definen el hardware y el software de red que puede necesitar.
- Lista de comprobación previa a la instalación que puede utilizar para anotar la configuración antes de configurar NetScaler Gateway.

Requisitos previos para instalar NetScaler Gateway

Antes de configurar la configuración en NetScaler Gateway, revise los siguientes requisitos previos:

- NetScaler Gateway está instalado físicamente en la red y tiene acceso a la red. NetScaler Gateway se implementa en la DMZ o en la red interna detrás de un firewall. También puede configurar NetScaler Gateway en una DMZ de doble salto y configurar conexiones a una comunidad de servidores. Citrix recomienda implementar el dispositivo en la DMZ.
- Puede configurar NetScaler Gateway con una puerta de enlace predeterminada o con rutas estáticas a la red interna para que los usuarios puedan acceder a los recursos de la red. NetScaler Gateway está configurado para usar rutas estáticas de forma predeterminada.
- Los servidores externos utilizados para la autenticación y autorización están configurados y en ejecución. Para obtener más información, consulte Autenticación y autorización.
- La red tiene un servidor de nombres de dominio (DNS) o un servidor del Servicio de nombres de Internet (WINS) de Windows para la resolución de nombres a fin de proporcionar la funcionalidad de usuario correcta de NetScaler Gateway.
- Ha descargado las licencias universales para las conexiones de usuario con el cliente Citrix Secure Access del sitio web de Citrix y las licencias están listas para instalarse en NetScaler Gateway.
- NetScaler Gateway tiene un certificado firmado por una entidad de certificación (CA) de confianza. Para obtener más información, consulte Instalar y administrar certificados.

Antes de instalar NetScaler Gateway, utilice la lista de comprobación previa a la instalación para anotar la configuración.

Planificación para la seguridad

Al planificar la implementación de NetScaler Gateway, debe comprender los problemas básicos de seguridad asociados con los certificados y con la autenticación y la autorización.

Configurar la administración segura de certificados

De forma predeterminada, NetScaler Gateway incluye un certificado de servidor Secure Sockets Layer (SSL) autofirmado que permite al dispositivo completar las conexiones SSL. Los certificados autofirmados son adecuados para realizar pruebas o para implementaciones de muestra, pero NetScaler no recomienda su uso en entornos de producción. Antes de implementar NetScaler Gateway en un entorno de producción, Citrix recomienda solicitar y recibir un certificado de servidor SSL firmado de una entidad de certificación (CA) conocida y cargarlo en NetScaler Gateway.

Si implementa NetScaler Gateway en cualquier entorno en el que NetScaler Gateway deba funcionar como cliente en un protocolo de enlace SSL (iniciar conexiones cifradas con otro servidor), también debe instalar un certificado raíz de confianza en NetScaler Gateway. Por ejemplo, si implementa NetScaler Gateway con Citrix Virtual Apps y la Interfaz Web, puede cifrar las conexiones de NetScaler Gateway a la Interfaz Web con SSL. En esta configuración, debe instalar un certificado raíz de confianza en NetScaler Gateway.

Soporte de autenticación

Puede configurar NetScaler Gateway para autenticar a los usuarios y controlar el nivel de acceso (o autorización) que tienen los usuarios a los recursos de red de la red interna.

Antes de implementar NetScaler Gateway, el entorno de red debe tener los directorios y los servidores de autenticación instalados para admitir uno de los siguientes tipos de autenticación:

- LDAP
- RADIUS
- TACACS+
- Certificado de cliente compatible con auditoría y tarjeta inteligente
- Configuración de RSA con RADIUS
- Autenticación SAML

Si su entorno no admite ninguno de estos tipos de autenticación o si tiene un número reducido de usuarios remotos, puede crear una lista de usuarios locales en NetScaler Gateway. A continuación,

puede configurar NetScaler Gateway para autenticar a los usuarios en esta lista local. Con esta configuración, no es necesario mantener las cuentas de usuario en un directorio externo independiente.

Proteja su implementación de NetScaler Gateway

Las distintas implementaciones pueden requerir distintas consideraciones de seguridad. Las directrices de implementación segura de NetScaler proporcionan una guía de seguridad general para ayudarlo a decidir cuál es la implementación segura adecuada en función de sus requisitos de seguridad específicos.

Para obtener más información, consulte las directrices de implementación segura de NetScaler.

Lista de comprobación previa a la instalación de gateway

January 26, 2024

La lista de comprobación consta de una lista de tareas e información de planificación que debe completar antes de instalar NetScaler Gateway.

Se proporciona espacio para que puedas marcar cada tarea a medida que la completes y hagas notas. Citrix recomienda tomar nota de los valores de configuración que debe introducir durante el proceso de instalación y durante la configuración de NetScaler Gateway.

Para ver los pasos para instalar y configurar NetScaler Gateway, consulte Instalación de NetScaler Gateway.

Dispositivos de usuario

- Asegúrese de que los dispositivos de usuario cumplan con los requisitos previos de instalación descritos en Requisitos del sistema de Citrix Secure Access
- Identificar los dispositivos móviles con los que se conectan los usuarios. **Nota**: Si los usuarios se conectan con un dispositivo iOS, debe habilitar Secure Browse en un perfil de sesión.

Conectividad básica de red NetScaler Gateway

Citrix recomienda obtener licencias y certificados de servidor firmados antes de empezar a configurar el dispositivo.

- Identifique y anote el nombre de host de NetScaler Gateway. **Nota**: Este no es el nombre de dominio completo (FQDN). El FQDN está contenido en el certificado de servidor firmado vinculado al servidor virtual.
- Obtenga licencias universales desde el sitio web de Citrix
- Genere una solicitud de firma de certificado (CSR) y envíela a una entidad de certificación (CA). Introduzca la fecha en que envía la CSR a la entidad emisora de certificados.
- Anote la dirección IP del sistema y la máscara de subred.
- Anote la dirección IP de la subred y la máscara de subred.
- Anote la contraseña de administrador. La contraseña predeterminada que viene con NetScaler Gateway es `nsroot`.
- Anote el número de puerto en el que NetScaler Gateway escucha las conexiones de usuario seguras. El valor predeterminado es el puerto TCP 443. Este puerto debe estar abierto en el firewall entre la red no segura (Internet) y la DMZ.
- Anote la dirección IP de la puerta de enlace predeterminada.
- Anote la dirección IP y el número de puerto del servidor DNS. El número de puerto predeterminado es 53. Además, si va a agregar el servidor DNS directamente, también debe configurar ICMP (ping) en el dispositivo.
- Anote la dirección IP y el nombre de host del primer servidor virtual.
- Anote la dirección IP y el nombre de host del segundo servidor virtual (si procede).
- Anote la dirección IP del servidor WINS (si procede).

Redes internas accesibles mediante NetScaler Gateway

- Anote las redes internas a las que los usuarios pueden acceder a través de NetScaler Gateway. Ejemplo: 10.10.0.0/24.
- Introduzca todas las redes internas y los segmentos de red a los que los usuarios necesitan acceder cuando se conectan a través de NetScaler Gateway mediante el cliente Citrix Secure Access.

Alta disponibilidad

Si tiene dos dispositivos NetScaler Gateway, puede implementarlos en una configuración de alta disponibilidad en la que un NetScaler Gateway acepta y administra las conexiones, mientras que un segundo NetScaler Gateway supervisa el primer dispositivo. Si el primer NetScaler Gateway deja de aceptar conexiones por cualquier motivo, el segundo NetScaler Gateway se hace cargo y comienza a aceptar conexiones de forma activa.

- Anote el número de versión del software de NetScaler Gateway.
- El número de versión debe ser el mismo en ambos dispositivos NetScaler Gateway.

- Anote la contraseña de administrador (`nsroot`). La contraseña debe ser la misma en ambos dispositivos.
- Anote la dirección IP y el ID principales de NetScaler Gateway. El número de identificación máximo es 64.
- Anote la dirección IP y el ID secundarios de NetScaler Gateway.
- Obtenga e instale la licencia universal en ambos dispositivos.
- Instale la misma licencia universal en ambos dispositivos.
- Anote la contraseña del nodo RPC.

Autenticación y autorización

NetScaler Gateway admite varios tipos de autenticación y autorización diferentes que se pueden utilizar en varias combinaciones. Para obtener información detallada sobre la autenticación y la autorización, consulte Autenticación y autorización.

Autenticación LDAP

Si su entorno incluye un servidor LDAP, puede utilizar LDAP para la autenticación.

- Anote la dirección IP y el puerto del servidor LDAP.

  Si permite conexiones no seguras con el servidor LDAP, el puerto predeterminado es 389. Si cifra las conexiones al servidor LDAP con SSL, el puerto predeterminado es 636.

- Anota el tipo de seguridad.

  Puede configurar la seguridad con o sin cifrado.

- Anote el DN de enlace de administrador.

  Si el servidor LDAP requiere autenticación, introduzca el DN de administrador que NetScaler Gateway debe usar para autenticarse al realizar consultas en el directorio LDAP. Un ejemplo es cn=administrator, cn=Users, dc=ace, dc=com.

- Anote la contraseña de administrador.

  La contraseña está asociada al DN de enlace de administrador.

- Anote el DN base.

  DN (o nivel de directorio) en el que se encuentran los usuarios; por ejemplo, ou=users, dc=ace, dc=com.

- Anote el atributo de nombre de inicio de sesión del servidor.

Introduzca el atributo de objeto persona del directorio LDAP que especifica el nombre de inicio de sesión de un usuario. El valor predeterminado es sAMAccountName. Si no utiliza Active Directory, los valores comunes de esta configuración son cn o uid.
Para obtener más información sobre la configuración del directorio LDAP, consulte Configuración de la autenticación LDAP

- Anota el atributo group.
  Introduzca el atributo de objeto persona del directorio LDAP que especifica los grupos a los que pertenece un usuario. El valor predeterminado es memberOf. Este atributo permite a NetScaler Gateway identificar los grupos de directorios a los que pertenece un usuario.
- Anote el nombre del subatributo.

Autorización y autenticación RADIUS

Si su entorno incluye un servidor RADIUS, puede utilizar RADIUS para la autenticación.
La autenticación RADIUS incluye productos RSA SecurID, SafeWord y Gemalto Protiva.

- Anote la dirección IP y el puerto del servidor RADIUS principal. El puerto predeterminado es 1812.
- Anote el secreto del servidor RADIUS principal (secreto compartido).
- Anote la dirección IP y el puerto del servidor RADIUS secundario. El puerto predeterminado es 1812.
- Anote el secreto del servidor RADIUS secundario (secreto compartido).
- Anote el tipo de codificación de contraseña (PAP, CHAP, MS-CHAP v1, MSCHAP v2).

Autenticación SAML

El lenguaje de marcado de aserciones de seguridad (SAML) es un estándar basado en XML para intercambiar autenticación y autorización entre proveedores de identidad (IdP) y proveedores de servicios.

- Obtenga e instale en NetScaler Gateway un certificado de proveedor de identidad seguro.
- Anota la URL de redireccionamiento.
- Anota el campo de usuario.
- Anote el nombre del certificado de firma.
- Anote el nombre del emisor de SAML.
- Anote el grupo de autenticación predeterminado.

Apertura de puertos a través de los firewalls (DMZ de salto único)

Si su organización protege la red interna con una única DMZ e implementa NetScaler Gateway en la DMZ, abra los siguientes puertos a través de los firewalls. Si va a instalar dos dispositivos NetScaler Gateway en una implementación DMZ de doble salto, consulte Abrir los puertos apropiados en los firewalls.

En el firewall entre la red no segura y la DMZ

- Abra un puerto TCP/SSL (predeterminado 443) en el firewall entre Internet y NetScaler Gateway. Los dispositivos de usuario se conectan a NetScaler Gateway en este puerto.

En el firewall entre la red segura

- Abra uno o más puertos apropiados en el firewall entre la DMZ y la red segura. NetScaler Gateway se conecta a uno o varios servidores de autenticación o a equipos que ejecutan Citrix Virtual Apps and Desktops en la red segura de estos puertos.
- Anote los puertos de autenticación.

  Abra solo el puerto adecuado para la configuración de NetScaler Gateway.

  - Para las conexiones LDAP, el valor predeterminado es el puerto TCP 389.
  - Para una conexión RADIUS, el valor predeterminado es el puerto UDP 1812. Anote los puertos de Citrix Virtual Apps and Desktops.
- Si utiliza NetScaler Gateway con Citrix Virtual Apps and Desktops, abra el puerto TCP 1494. Si habilita la fiabilidad de la sesión, abra el puerto TCP 2598 en lugar del 1494. Citrix recomienda mantener abiertos estos dos puertos.

Citrix Virtual Desktops, Citrix Virtual Apps, la Interfaz Web o StoreFront

Realice las siguientes tareas si va a implementar NetScaler Gateway para proporcionar acceso a Citrix Virtual Apps and Desktops a través de la Interfaz Web o StoreFront. El cliente Citrix Secure Access no es necesario para esta implementación. Los usuarios acceden a aplicaciones y escritorios publicados a través de NetScaler Gateway mediante únicamente exploradores web y Citrix Receiver.

- Anote el FQDN o la dirección IP del servidor que ejecuta la Interfaz Web o StoreFront.
- Anote el FQDN o la dirección IP del servidor que ejecuta Secure Ticket Authority (STA) (solo para Interfaz Web).

Citrix Endpoint Management

Realice las siguientes tareas si implementa Citrix Endpoint Management en su red interna. Si los usuarios se conectan a Endpoint Management desde una red externa, como Internet, los usuarios deben conectarse a NetScaler Gateway antes de acceder a las aplicaciones móviles, web y SaaS.

- Anote el FQDN o la dirección IP de Endpoint Management.
- Identificar aplicaciones web, SaaS y móviles iOS o Android a las que pueden acceder los usuarios.

Implementación de DMZ de doble salto con Citrix Virtual Apps

Realice las siguientes tareas si va a implementar dos dispositivos NetScaler Gateway en una configuración DMZ de doble salto para admitir el acceso a los servidores que ejecutan Citrix Virtual Apps.

NetScaler Gateway en la primera DMZ

La primera DMZ es la DMZ en el extremo exterior de la red interna (la más cercana a Internet o la red no segura). Los clientes se conectan a NetScaler Gateway en la primera DMZ a través del firewall que separa Internet de la DMZ. Recopile esta información antes de instalar NetScaler Gateway en la primera DMZ.

- Complete los elementos de la sección Conectividad de red básica de NetScaler Gateway de esta lista de comprobación para NetScaler Gateway.

  Al completar estos elementos, la Interfaz 0 conecta este NetScaler Gateway a Internet y la Interfaz 1 conecta este NetScaler Gateway a NetScaler Gateway en la segunda DMZ.

- Configure la información del segundo dispositivo DMZ en el dispositivo principal.

  Para configurar NetScaler Gateway como primer salto de la DMZ de doble salto, debe especificar el nombre de host o la dirección IP de NetScaler Gateway en la segunda DMZ del dispositivo en la primera DMZ. Después de especificar cuándo se configura el proxy de NetScaler Gateway en el dispositivo en el primer salto, enlaza a NetScaler Gateway de forma global o a un servidor virtual.

- Anote el protocolo de conexión y el puerto entre dispositivos.

  Para configurar NetScaler Gateway como primer salto de la doble DMZ, debe especificar el protocolo de conexión y el puerto en el que NetScaler Gateway de la segunda DMZ escucha las conexiones. El protocolo de conexión y el puerto son SOCKS con SSL (puerto predeterminado 443). El protocolo y el puerto deben estar abiertos a través del firewall que separa la primera DMZ y la segunda DMZ.

NetScaler Gateway en la segunda DMZ

La segunda DMZ es la DMZ más cercana a su red interna y segura. NetScaler Gateway implementado en la segunda DMZ sirve como proxy para el tráfico ICA, atravesando la segunda DMZ entre los dispositivos de usuario externos y los servidores de la red interna.

- Complete las tareas de la sección Conectividad de red básica de NetScaler Gateway de esta lista de comprobación para NetScaler Gateway.

  Al completar estos elementos, la Interfaz 0 conecta este NetScaler Gateway a NetScaler Gateway en la primera DMZ. La interfaz 1 conecta este NetScaler Gateway a la red segura.

Instalación y configuración del dispositivo NetScaler Gateway

January 26, 2024

Cuando recibe el dispositivo NetScaler Gateway, desempaqueta el dispositivo y prepara el sitio y el bastidor. Una vez que determine que la ubicación en la que instala el dispositivo cumple con los estándares medioambientales y que el bastidor de servidores está instalado de acuerdo con las instrucciones, instale el hardware. Después de montar el dispositivo, lo conecta a la red, a una fuente de alimentación y al terminal de consola que utiliza para la configuración inicial. Después de encender el dispositivo, realiza la configuración inicial y asigna direcciones IP de administración y de red. Asegúrese de observar las precauciones y advertencias enumeradas con las instrucciones de instalación.

Al instalar un dispositivo virtual NetScaler VPX, primero debe adquirir la imagen del dispositivo virtual e instalarla en un hipervisor u otro monitor de máquina virtual.

Citrix recomienda utilizar el tema Lista de comprobación previa a la instalación de NetScaler Gateway para que pueda tomar nota de la configuración antes de intentar configurar un dispositivo NetScaler Gateway. La lista de comprobación incluye información sobre la instalación de NetScaler Gateway y un dispositivo.

Configurar el dispositivo NetScaler Gateway mediante asistentes

March 27, 2024

NetScaler Gateway tiene los seis asistentes siguientes que puede utilizar para configurar los ajustes del dispositivo:

- El asistente de configuración por primera vez aparece cuando inicia sesión en el dispositivo NetScaler Gateway por primera vez.
- El asistente de configuración rápida le ayuda a configurar las directivas, expresiones y opciones correctas para las conexiones a Citrix Endpoint Management, StoreFront y la Interfaz Web.
- El asistente de NetScaler Gateway le ayuda a configurar la configuración específica de NetScaler Gateway.
- El asistente de configuración le ayuda a configurar los ajustes básicos de NetScaler Gateway por primera vez.
- La configuración integrada de Citrix Endpoint Management le ayuda a configurar el entorno de NetScaler Gateway y Citrix Endpoint Management.
- El asistente Aplicaciones publicadas le ayuda a configurar los ajustes de las conexiones de usuario mediante la aplicación Citrix Workspace.

Asistente de configuración por primera vez

Cuando termina de instalar y configurar la configuración inicial en el dispositivo NetScaler Gateway, cuando inicia sesión en la utilidad de configuración por primera vez, aparece el Asistente de configuración por primera vez si no se cumplen las siguientes condiciones:

- No ha instalado una licencia en el dispositivo.
- No ha configurado una subred ni una dirección IP asignada.
- Si la dirección IP predeterminada de los dispositivos es 192.168.100.1.

Configurar NetScaler Gateway con el asistente de configuración por primera vez

Para configurar NetScaler Gateway (el dispositivo físico o el dispositivo virtual VPX) por primera vez, necesita un equipo administrativo configurado en la misma red que el dispositivo.

Asigne una dirección IP de NetScaler Gateway (NSIP) como dirección IP de administración del dispositivo y una dirección IP de subred (SNIP) a la que se puedan conectar los servidores. Asigne una máscara de subred que se aplica tanto a las direcciones de NetScaler Gateway como a las SNIP. Configure también una zona horaria. Si asigna un nombre de host, puede acceder al dispositivo especificando su nombre en lugar de la dirección NSIP.

Hay dos secciones en el Asistente de configuración por primera vez. En la primera sección, se configuran las opciones básicas del sistema para el dispositivo NetScaler Gateway, que incluyen:

Dirección NSIP, dirección SNIP y máscara de subred Nombre de host del
equipo Servidores
DNS Zona
horaria Contraseña del

administrador
En la segunda sección, se instalan las licencias. Si especifica la dirección de un servidor DNS, puede utilizar el número de serie de hardware (HSN) o la clave de licencia para asignar las licencias, en lugar de cargar las licencias desde un equipo local al dispositivo.

Nota: Citrix recomienda guardar las licencias en el equipo local.

Cuando termine de configurar estos valores, NetScaler Gateway le pedirá que reinicie el dispositivo. Cuando vuelva a iniciar sesión en el dispositivo, puede utilizar otros asistentes y la utilidad de configuración para configurar otras opciones.

Asistente de configuración rápida

El asistente de configuración rápida le permite configurar varios servidores virtuales en NetScaler Gateway. Puede agregar, modificar y quitar servidores virtuales.

El asistente de configuración rápida permite una configuración perfecta para las siguientes implementaciones:

- Conexiones de la Interfaz Web a Citrix Virtual Apps and Desktops, con la capacidad de configurar varias instancias de Secure Ticket Authority (STA)
- Solo Citrix Endpoint Management
- Solo StoreFront
- Citrix Endpoint Management y StoreFront juntos

El asistente de configuración rápida le permite configurar las siguientes opciones en el dispositivo:

- Nombre del servidor virtual, dirección IP y puerto
- Redirección de un puerto no seguro a un puerto seguro
- Servidor LDAP
- Servidor RADIUS
- Certificados
- Servidor DNS
- Citrix Endpoint Management y Citrix Virtual Apps and Desktops

  Nota: Para habilitar el inicio de sesión único, debe habilitar manualmente la opción Inicio de **sesión único en aplicaciones web** en la ficha **Crear perfil de sesión de NetScaler Gateway > Experiencia del cliente** para la acción de sesión.

NetScaler Gateway admite conexiones de usuario directamente con Citrix Endpoint Management, lo que proporciona a los usuarios acceso a sus aplicaciones web, SaaS y móviles, además de acceso a

ShareFile. También puede configurar la configuración de StoreFront, lo que permite a los usuarios acceder a sus aplicaciones y escritorios virtuales basados en Windows.

Al ejecutar el Asistente de configuración rápida, se crean las siguientes directivas en función de la configuración de Citrix Endpoint Management, StoreFront e Interfaz Web:

- Directivas de sesión, incluidas directivas y perfiles para Receiver, Receiver for Web, el cliente Citrix Secure Access y Program Neighborhood Agent
- Acceso sin cliente
- Autenticación LDAP y RADIUS

Configure los ajustes con el asistente de configuración rápida

Puede configurar la configuración en NetScaler Gateway para habilitar la comunicación con Citrix Endpoint Management, StoreFront o la Interfaz Web mediante el Asistente de configuración rápida. Al completar la configuración, el asistente crea las directivas correctas para la comunicación entre NetScaler Gateway, Endpoint Management, StoreFront o la Interfaz Web. Estas directivas incluyen directivas de autenticación, sesión y acceso sin cliente. Cuando finaliza el asistente, las directivas se enlazan al servidor virtual.

Al completar el asistente de configuración rápida, NetScaler Gateway puede comunicarse con Endpoint Management o StoreFront, y los usuarios pueden acceder a sus aplicaciones basadas en Windows y escritorios virtuales y aplicaciones web, SaaS y móviles. Los usuarios pueden conectarse directamente a Endpoint Management.

Durante el asistente, se configuran las siguientes opciones:

- Nombre del servidor virtual, dirección IP y puerto
- Redirección de un puerto no seguro a un puerto seguro
- Certificados
- Servidor LDAP
- Servidor RADIUS
- Certificado de cliente para autenticación (solo para autenticación de dos factores)
- Endpoint Management, StoreFront o Interfaz Web

El asistente de configuración rápida admite la autenticación de certificados de cliente, LDAP y RADIUS. Puede configurar la autenticación de dos factores en el asistente siguiendo estas pautas:

- Si selecciona LDAP como tipo de autenticación principal, puede configurar RADIUS como tipo de autenticación secundaria.
- Si selecciona RADIUS como tipo de autenticación principal, puede configurar LDAP como tipo de autenticación secundaria.

- Si selecciona certificados de cliente como tipo de autenticación principal, puede configurar LDAP o RADIUS como tipo de autenticación secundaria.

No se pueden crear varias directivas de autenticación LDAP mediante el Asistente de configuración rápida. Por ejemplo, quiere configurar una directiva que utilice SAMAccountName en el campo **Atributo de nombre de inicio de sesión del servidor** y una segunda directiva LDAP que utilice el nombre principal de usuario (UPN) en el campo **Atributo de nombre de inicio de sesión del servidor**. Para configurar estas directivas independientes, utilice la utilidad de configuración de NetScaler Gateway para crear las directivas de autenticación. Para obtener más información, consulte Configuración de la autenticación LDAP.

Puede configurar certificados para NetScaler Gateway en el Asistente de configuración rápida mediante los métodos siguientes:

- Seleccione un certificado instalado en el dispositivo.
- Instale un certificado y una clave privada.
- Seleccione un certificado de prueba.
  Nota: Si usa un certificado de prueba, debe agregar el nombre de dominio completo (FQDN) que figura en el certificado.

Puede abrir el **Asistente de configuración rápida** de una de las dos formas siguientes:

- Cuando se encuentra en la página de inicio de sesión de NetScaler Gateway y seleccione **NetScaler Gateway** en **Tipo de implementación**, aparece la ficha **Inicio**. Si selecciona cualquier otra opción en **Tipo de implementación**, la ficha **Inicio** no aparece.
- Desde el enlace **Crear/supervisar NetScaler Gateway** del panel de detalles de NetScaler Gateway. El enlace aparece si instala una licencia que habilita las funciones de NetScaler. Si otorga la licencia del dispositivo solo para NetScaler Gateway, el enlace no aparece.

Después de ejecutar el asistente por primera vez, puede volver a ejecutarlo para crear más servidores virtuales y configuraciones.

Importante: Si utiliza el Asistente de configuración rápida para configurar un servidor virtual NetScaler Gateway adicional, debe utilizar una dirección IP única. No se puede utilizar la misma dirección IP que se utiliza en un servidor virtual existente. Por ejemplo, tiene un servidor virtual con la dirección IP 192.168.10.5 con un número de puerto 80. Ejecute el Asistente de configuración rápida para crear un segundo servidor virtual con la dirección IP 192.168.10.5 con el número de puerto 443. Al intentar guardar la configuración, se produce un error.

Para configurar los ajustes con el asistente de configuración rápida

1. En la utilidad de configuración, realice una de las siguientes acciones:
   a) Si el dispositivo solo tiene licencia para NetScaler Gateway, haga clic en la ficha **Inicio**.

b) Si el dispositivo tiene licencia para incluir funciones de NetScaler, en la ficha Configuración, en el panel de navegación, haga clic en **NetScaler Gateway** y, a continuación, en el panel de detalles, en **Introducción**, haga clic en **Configurar NetScaler Gateway para Enterprise Store**.

2. En el panel de control, haga clic en **Crear nuevo NetScaler Gateway**.
3. En **Configuración de NetScaler Gateway**, configure lo siguiente:

   a) En **Nombre**, escriba un nombre para el servidor virtual.
   b) En **Dirección IP**, escriba la dirección IP del servidor virtual.
   c) En **Puerto**, escriba el número de puerto. El número de puerto predeterminado es 443.
   d) Seleccione Redirigir solicitudes desde el puerto 80 al puerto seguro para permitir que las conexiones de usuario del puerto 80 vayan al puerto 443.

4. Haga clic en **Continuar**.
5. En la página Certificado, realice una de las siguientes acciones:

   a) Haga clic en **Elegir certificado** y, a continuación, en Certificado, seleccione el certificado.
   b) Haga clic en **Instalar certificado y,** a continuación, en **Elegir certificado** y en **Elegir clave**, haga clic en **Examinar** para desplazarse hasta el certificado y la clave privada.
   c) Haga clic en **Usar certificado de prueba** y, a continuación, en FQDN de certificado, introduzca el nombre de dominio completo (FQDN) contenido en el certificado de prueba.

6. Haga clic en **Continuar**.
7. En Configuración de autenticación, haga lo siguiente:

   a) En **Autenticación primaria**, seleccione LDAP, RADIUS o Cert.
   b) Seleccione un servidor de autenticación o configure la configuración del tipo de autenticación que seleccionó en el paso anterior. Si selecciona Cert, seleccione el certificado de cliente o instale un nuevo certificado de cliente.
   c) En **Autenticación secundaria**, seleccione el tipo de autenticación y, a continuación, configure la configuración del servidor de autenticación.

8. Haga clic en **Continuar**.

Cuando termine de configurar los ajustes de red y autenticación, podrá configurar los ajustes de Citrix Endpoint Management o Citrix Virtual Apps and Desktops (StoreFront o Interfaz Web).

Configurar los ajustes de almacén empresarial NetScaler Gateway admite el acceso de los usuarios a aplicaciones web, SaaS y móviles y ShareFile solo a través de Endpoint Management. Si también implementa StoreFront o la Interfaz Web, los usuarios tienen acceso a aplicaciones y escritorios virtuales basados en Windows. Puede configurar los ajustes de las siguientes opciones:

- Solo Endpoint Management

- Solo StoreFront
- Endpoint Management y StoreFront juntos
- Solo Interfaz Web

Al hacer clic en **Continuar** del procedimiento anterior, podrá configurar los ajustes de su caso de implementación. Los siguientes procedimientos se inician en la página Configuración de integración de Citrix.

Después de crear el servidor virtual, modificar el servidor virtual en el Asistente de configuración rápida no le permite cambiar la configuración de Citrix Endpoint Management o Citrix Virtual Apps and Desktops.

Por ejemplo, si cancela la configuración de un servidor virtual en cualquier etapa antes de configurar los ajustes de **Citrix Enterprise Store**, el asistente selecciona automáticamente la Interfaz Web sin configurar ninguna configuración. Cuando se produce esta situación, puede modificar los detalles del servidor virtual para configurar la Interfaz Web, pero no puede cambiar a Citrix Endpoint Management. Para cambiar, debe crear un nuevo servidor virtual y no debe cancelar el asistente en ningún momento durante la configuración. Si no necesita el servidor virtual de Interfaz Web, puede eliminarlo mediante el Asistente de configuración rápida.

Para configurar las opciones solo para StoreFront

1. Haga clic en **Citrix Virtual Apps and Desktops**.
2. En **Tipo de implementación**, seleccione **StoreFront**.
3. En el **FQDN de StoreFront**, introduzca el nombre de dominio completo (FQDN) del servidor StoreFront.
4. En **Receiver para Web Path**, deje la ruta predeterminada o introduzca la suya propia.
5. Seleccione **HTTPS** para proteger las conexiones de usuario.
6. En **Dominio de inicio de sesión único**, introduzca el dominio de StoreFront.
7. En **URL de STA**, introduzca la dirección IP completa o el FQDN del servidor que ejecuta Secure Ticket Authority (STA) si implementa StoreFront y proporciona acceso a aplicaciones publicadas desde Citrix Virtual Apps o escritorios virtuales desde Citrix Virtual Desktops.
8. Haga clic en **Listo**.

Cuando los usuarios se conectan a StoreFront a través de NetScaler Gateway, los usuarios pueden iniciar sus aplicaciones y escritorios desde Receiver para Web o Receiver.

Para configurar valores solo para Endpoint Management

1. Haga clic en **Citrix Endpoint Management**.
2. En el **FQDN de App Controller**, introduzca el FQDN de Endpoint Management.
3. Haga clic en **Listo**.

Para configurar los ajustes de la Interfaz Web

1. En el asistente de configuración rápida, haga clic en **Citrix Virtual Apps and Desktops**.
2. En **Tipo de implementación**, seleccione **Interfaz web**y, a continuación, configure lo siguiente:
    a) En **URL del sitio de Citrix Virtual Apps**, escriba la dirección IP completa o el FQDN de la Interfaz Web.
    b) En la **URL del sitio de Citrix Virtual Apps Services**, escriba la dirección IP completa o el FQDN de la interfaz web con la ruta de la aplicación Citrix Workspace. Puede introducir la ruta por defecto o introducir su propia ruta.
    c) En **Dominio de inicio de sesión único**, introduzca el dominio que va a utilizar.
    d) En **URL de STA**, escriba la dirección IP completa o el FQDN del servidor que ejecuta STA.
3. Haga clic en **Listo**.

Asistente de NetScaler Gateway

Utilice el asistente de NetScaler Gateway para configurar la siguiente configuración en el dispositivo:

- Servidores virtuales
- Certificados
- Proveedores de servicios de nombres
- Autenticación
- Autorización
- Redirección de puertos
- Acceso sin cliente
- Acceso sin cliente para SharePoint

Configurar ajustes mediante el asistente de NetScaler Gateway

Después de ejecutar el Asistente de configuración, puede ejecutar el asistente de NetScaler Gateway para configurar otras opciones en NetScaler Gateway. Ejecute el asistente de NetScaler Gateway desde la utilidad de configuración.

NetScaler Gateway incluye un certificado de prueba. Si no tiene un certificado firmado de una entidad emisora de certificados (CA), puede usar el certificado de prueba al utilizar el asistente de NetScaler Gateway. Cuando reciba el certificado firmado, puede quitar el certificado de prueba e instalar el certificado firmado. Citrix recomienda obtener el certificado firmado antes de poner NetScaler Gateway a disposición del público para los usuarios.

Nota: Puede crear una solicitud de firma de certificado (CSR) desde el asistente de NetScaler Gateway. Si utiliza el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y volver a

iniciarlo cuando reciba el certificado firmado de la entidad emisora de certificados. Para obtener más información sobre los certificados, consulte
Instalación y administración de certificados.

Puede configurar las conexiones de usuario para el protocolo de Internet versión 6 (IPv6) en el asistente de NetScaler Gateway cuando configura un servidor virtual. Para obtener más información sobre el uso de IPv6 para las conexiones de usuario, consulte Configuración de IPv6 para conexiones de usuario.

Para iniciar el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente de NetScaler Gateway .
3. Haga clic en Next y siga las instrucciones del asistente.

Asistente de configuración

Utilice el Asistente de configuración para configurar la siguiente configuración inicial en el dispositivo:

- Dirección IP del sistema y máscara de subred
- Dirección IP asignada y máscara de subred
- Nombre de host
- Puerta de enlace predeterminada
- Licencias

Nota: Antes de ejecutar el Asistente de configuración, descargue las licencias del sitio web de Citrix. Para obtener más información, consulte
Licencias de NetScaler Gateway

Asistente para aplicaciones publicadas

Utilice el asistente Aplicaciones publicadas para configurar NetScaler Gateway para que se conecte a los servidores que ejecutan Citrix Virtual Apps and Desktops en la red interna. Con el asistente Aplicaciones publicadas, puede:

- Seleccione un servidor virtual para las conexiones a la comunidad de servidores.
- Configure la configuración de las conexiones de usuario para la Interfaz Web o StoreFront, el inicio de sesión único y Secure Ticket Authority.
- Cree o seleccione directivas de sesión para SmartAccess.

En el asistente, también puede crear expresiones de directivas de sesión para conexiones de usuario. Para obtener más información sobre cómo configurar NetScaler Gateway para conectarse a un conjunto de servidores, consulte Proporcionar acceso a aplicaciones publicadas y escritorios virtuales a través de la Interfaz Web.

Configuración integrada de Citrix Endpoint Management

Puede implementar NetScaler Gateway con MDM de Citrix Endpoint Management, que ofrece la capacidad de escalar, garantizar la alta disponibilidad de las aplicaciones y mantener la seguridad. Para utilizar la configuración de Citrix Endpoint Management, debe instalar la versión 10.1, compilación 120.1316.e.

La configuración integrada de Citrix Endpoint Management crea lo siguiente:

- Servidores de equilibrio de carga para Device Manager.
- Servidores de equilibrio de carga para Microsoft Exchange con filtrado de correo electrónico.
- Servidores de equilibrio de carga para ShareFile.

Para obtener más información sobre cómo crear ajustes con la configuración integrada de Citrix Endpoint Management, consulte Configuración de las opciones del entorno de Citrix Endpoint Management

Configurar NetScaler Gateway

January 26, 2024

Después de configurar la configuración de red básica en NetScaler Gateway, configure la configuración detallada para que los usuarios puedan conectarse a los recursos de red de la red segura. Esta configuración incluye:

- Servidores virtuales. Puede configurar varios servidores virtuales en NetScaler Gateway, lo que le permite crear directivas diferentes según el caso de usuario que deba implementar. Cada servidor virtual tiene su propia dirección IP, certificado y conjunto de directivas. Por ejemplo, puede configurar un servidor virtual y restringir a los usuarios a los recursos de red de la red interna en función de su pertenencia a grupos y de las directivas que vincule a los servidores virtuales. Puede crear servidores virtuales mediante los métodos siguientes:
  - Asistente de configuración rápida
  - Asistente de NetScaler Gateway
  - Utilidad de configuración

- Alta disponibilidad. Puede configurar la alta disponibilidad cuando implementa dos dispositivos NetScaler Gateway en la red. Si los dispositivos principales fallan, el dispositivo secundario puede asumir el control sin afectar a las sesiones del usuario.
- Certificados. Puede utilizar certificados para proteger las conexiones de los usuarios con NetScaler Gateway. Al crear una solicitud de firma de certificado (CSR), agrega el nombre de dominio completo al certificado. Puede enlazar certificados a servidores virtuales.
- Autenticación. NetScaler Gateway admite varios tipos de autenticación, incluidos LDAP local, RADIUS, SAML, certificados de cliente y TACACS+. Además, puede configurar la autenticación en cascada y en dos fases.
  Nota: Si utiliza RSA, Safeword o Gemalto Protiva para la autenticación, configure estos tipos mediante RADIUS.
- Conexiones de usuarios. Puede configurar las conexiones de usuario mediante perfiles de sesión. Dentro del perfil, puede determinar los plug-ins con los que los usuarios pueden iniciar sesión, junto con cualquier restricción que los usuarios puedan necesitar. A continuación, puede crear una directiva con un perfil. Puede enlazar directivas de sesión a usuarios, grupos y servidores virtuales.
- Página de inicio. Puede utilizar la interfaz de acceso predeterminada como página de inicio o crear una página principal personalizada. La página principal aparece después de que los usuarios inicien sesión correctamente en NetScaler Gateway.
- Análisis de endpoints. Puede configurar directivas en NetScaler Gateway que comprueban el dispositivo del usuario en busca de software, archivos, entradas de registro, procesos y sistemas operativos cuando los usuarios inician sesión. El análisis de puntos finales le permite aumentar la seguridad de su red al exigir que el dispositivo del usuario cuente con el software necesario.

Uso de la utilidad de configuración

La utilidad de configuración permite configurar la mayoría de los parámetros de NetScaler Gateway. Utiliza un explorador web para acceder a la utilidad de configuración.

Inicie sesión en la utilidad de configuración

1. En un explorador web, escriba la dirección IP del sistema de NetScaler Gateway, como `http://192.168.100.1`.
   Nota: NetScaler Gateway está preconfigurado con una dirección IP predeterminada de 192.168.100.1 y una máscara de subred
   255.255.0.0.
2. En Nombre de usuario y contraseña, escriba `nsroot`.
3. En Tipo de implementación, seleccione NetScaler Gateway y luego haga clic en Iniciar sesión.

Al iniciar sesión en la utilidad de configuración por primera vez, el panel se abre de forma predeterminada en la ficha **Inicio**. En la ficha **Inicio**, puede utilizar el Asistente de configuración rápida para configurar la configuración de un servidor virtual, autenticación, certificados y Citrix Endpoint Management. También puede configurar los valores de StoreFront o de Interfaz Web en el Asistente de configuración rápida.

Para obtener más información sobre la configuración de NetScaler Gateway, consulte:

- Configuración de los ajustes iniciales mediante el Asistente de configuración.
- Configurar parámetros con el Asistente de configuración rápida
- Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

Creación de servidores virtuales

March 27, 2024

Un servidor virtual es un punto de acceso en el que los usuarios inician sesión. Cada servidor virtual tiene su propia dirección IP, certificado y conjunto de directivas. Un servidor virtual consiste en una combinación de dirección IP, puerto y protocolo que acepta tráfico entrante. Los servidores virtuales contienen la configuración de conexión para cuando los usuarios inician sesión en el dispositivo. Puede configurar los siguientes ajustes en los servidores virtuales:

- Certificados
- Autenticación
- Directivas
- Marcadores
- Grupos de direcciones (también conocidos como grupos de IP o IP de intranet)
- Implementación DMZ de doble salto con NetScaler Gateway
- Secure Tíquet Authority
- Transferencia de sesión proxy ICA SmartAccess

Si ejecuta el asistente de NetScaler Gateway, puede crear un servidor virtual durante el asistente. Puede configurar más servidores virtuales de las siguientes formas:

- **Desde el nodo servidores virtuales**. Este nodo se encuentra en el panel de navegación de la utilidad de configuración. Puede agregar, modificar y quitar servidores virtuales mediante la utilidad de configuración.
- **Con el asistente de configuración rápida**. Si implementa Citrix Endpoint Management, StoreFront o la Interfaz Web en su entorno, puede utilizar el Asistente de configuración rápida para crear el servidor virtual y todas las directivas necesarias para su implementación.

Si quiere que los usuarios inicien sesión y utilicen un tipo de autenticación específico, como RADIUS, puede configurar un servidor virtual y asignar al servidor una dirección IP única. Cuando los usuarios inician sesión, se les dirige al servidor virtual y, a continuación, se les solicitan sus credenciales RADIUS.

También puede configurar las formas en que los usuarios inician sesión en NetScaler Gateway. Puede utilizar una directiva de sesión para configurar el tipo de software de usuario, el método de acceso y la página principal que ven los usuarios tras iniciar sesión.

Para crear servidores virtuales

Puede agregar, modificar, habilitar o inhabilitar y quitar servidores virtuales mediante la GUI de NetScaler Gateway o el asistente de configuración rápida. Para obtener más información sobre cómo configurar un servidor virtual con el Asistente de configuración rápida, consulte Configuración de valores con el Asistente de configuración rápida.

> **Nota:**
>
> El servidor virtual VPN admite la versión 1.0 de DTLS de forma predeterminada. Para habilitar la versión 1.2 de DTLS, consulte Configurar el servidor virtual VPN DTLS mediante un servidor virtual VPN SSL.

Servidor virtual HTTP QUIC VPN

A partir de la versión 14.1, compilación 8.x, NetScaler Gateway admite el uso de HTML5 en el explorador para enviar tráfico ICA mediante QUIC e iniciar sesiones de Citrix DaaS. Puede crear un servidor virtual de VPN de tipo de servicio HTTP QUIC para lanzar aplicaciones Citrix DaaS a través de QUIC en clientes HTML5, sin necesidad de un software de plug-in de cliente. Anteriormente, las aplicaciones Citrix DaaS tenían que iniciarse a través de exploradores web que utilizaran el software del plug-in de cliente de la aplicación Citrix Workspace o aplicaciones cliente HTML5 mediante WebSockets (acceso sin cliente).

Los clientes HTML5 admiten el protocolo WebTransport. El protocolo WebTransport usa HTTP3 sobre QUIC para establecer la comunicación entre un cliente y un servidor web. Para obtener más información sobre HTTP a través de QUIC, consulte Protocolo HTTP a través de QUIC.

Configurar el servidor virtual HTTP QUIC VPN mediante la GUI

1. Configure el servidor virtual HTTP QUIC VPN.
    a) Vaya a **Configuración > NetScaler Gateway > Servidores virtuales**.
    b) En la página **Servidores virtuales de NetScaler Gateway**, haga clic en **Agregar**.

c) En **Protocolo**, seleccione **HTTP_QUIC**.

d) Actualice los campos restantes según sea necesario y haga clic en **Aceptar**.

2. Habilite HTTP/3 WebTransport en el perfil HTTP.

   - Vaya a **Sistema > Perfiles > Perfiles HTTP**. En la sección **HTTP/3**, active la casilla **HTTP/3** WebTransport. Para obtener más información sobre los perfiles HTTP, consulte Configuraciones HTTP.

Configure el servidor virtual HTTP QUIC VPN mediante la CLI

1. Configure un servidor virtual de VPN del tipo de servicio `HTTP QUIC`.

```
add vpn vserver <VPN server name> -service type <HTTP_QUIC> -dtls
    <off> -Listenpolicy <NONE> -httpProfileName <name of the HTTP
    QUIC profile> -deploymentType <ICA_STOREFRONT> -vserverFqdn <
    URL>
<!--NeedCopy-->
```

2. Habilite HTTP/3 WebTransport en el perfil HTTP.

```
set httpprofile nshttp_default_http_quic_profile -http3webTransport
 ENABLED
```

El resultado del siguiente comando show muestra el parámetro `HTTP/3 WebTransport: ENABLED`. Este parámetro indica que el tipo de servicio `HTTP QUIC` se utiliza para enviar tráfico de WebTransport entre el cliente y el servidor virtual de VPN.

```
sh httpprofile <name>

HTTP/2 Strict Cipher: ENABLED
        HTTP/3: ENABLED
        HTTP/3 maximum header field section size: 24576
        HTTP/3 maximum header table size: 4096
        HTTP/3 maximum header blocked streams: 100
        HTTP/3 WebTransport: ENABLED
        gRPC Buffer Limit: 131072
        gRPC Buffer Timeout: 1000
        gRPC Length Delimited Message: ENABLED
        Apdex Client Response Threshold: 500
        HTTP pipeline req buffer size: 131072
        Reference count: 2

<!--NeedCopy-->
```

> **Notas:**
>
> - La dirección IP y el número de puerto deben ser los mismos para los servidores virtuales

> SSL y HTTP QUIC VPN. Sin embargo, el DTLS debe estar inhabilitado en el servidor virtual de VPN con SSL porque no puede ejecutar tanto DTLS como HTTP_QUIC en una dirección IP y un número de puerto comunes. Para obtener más información sobre el servidor virtual de VPN de DTLS, consulte Configurar el servidor virtual de VPN de DTLS mediante el servidor virtual de VPN de SSL.
> - El perfil HTTP configurado con el valor de servicio alternativo establecido en `Altsvc=h3=":port number"` debe estar enlazado al servidor virtual de VPN con SSL. Para obtener más información sobre el parámetro Alternative Service, consulte HTTP/2 para configurar el equilibrio de cargas HTTP.

Para crear un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. En el panel de detalles, haga clic en **Agregar**.
3. Configure los ajustes según sus necesidades.
4. Haga clic en **Create** y, luego, en **Close**.

Para crear un servidor virtual mediante la CLI

En la línea de comandos, escriba;

```
add vpn vserver <name> <serviceType> [<IPAddress> <port>]
<!--NeedCopy-->
```

Ejemplo:

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
<!--NeedCopy-->
```

Puntos a tener en cuenta al enlazar un perfil de red al servidor virtual de VPN

Puede crear perfiles de red (perfiles de red) para configurar el dispositivo de modo que utilice una dirección IP de origen especificada y vincular el perfil de red al servidor virtual de VPN. Sin embargo, tenga en cuenta lo siguiente al vincular un perfil de red al servidor virtual de VPN.

- Al enlazar un perfil de red a un servidor virtual de NetScaler Gateway, el perfil de red no selecciona un SNIP específico para que lo utilice el servidor virtual o el servicio para el tráfico a los servidores back-end. En su lugar, el dispositivo de puerta de enlace ignora el enlace del perfil de red y utiliza el método round robin para seleccionar los SNIP.
- El perfil de red no funciona para los servicios generados dinámicamente (STA, monitor SF). Para STA y otros servicios generados dinámicamente, puede enlazar el perfil de red a esos monitores

directamente y esos monitores se utilizarán en ese momento. Sin embargo, si tiene varias puertas de enlace en el mismo dispositivo, todas las puertas de enlace utilizan el mismo perfil de red para los monitores configurados.

Para obtener más información sobre el perfil de red, consulte Usar una IP de origen especificada para la comunicación back-end.

Dirección IP de origen del perfil de red en una configuración de servidor virtual VPN DTLS para el lanzamiento de UDP

A partir de la versión 14.1, compilación 17.38, NetScaler Gateway configurado con DTLS Listener elige la dirección IP de origen del perfil de red para establecer una conexión UDP con el Virtual Delivery Agent (VDA). Asegúrese de que el perfil de red esté enlazado al servidor virtual VPN SSL.

Ejecute los siguientes comandos de la CLI para configurar un perfil de red en el servidor virtual VPN:

```
add ip <IPAddress><netmask> -type SNIP
add netprofile net1 -srcIP <IPAddress>
set vpn vserver <name> -netProfile net1
<!--NeedCopy-->
```

Para verificar si se usa la dirección IP de origen elegida, ejecute el comando de la CLI `show connectiontable`.

Usuarios actuales y usuarios conectados totales en el servidor virtual

Usuarios actuales: número de usuarios que han iniciado sesión en un servidor virtual específico. Se recomienda supervisar a los usuarios actuales para el seguimiento de las CCUs.

Total de usuarios conectados: número de usuarios que tienen una o más conexiones activas a través del servidor virtual específico. El número total de usuarios conectados se utiliza principalmente en ICA Proxy.

Puede utilizar el contador de número total de usuarios conectados en los siguientes casos:

- Tenga en cuenta que se ha establecido una conexión ICA pero no se ha establecido ninguna sesión de autenticación, autorización ni auditoría correspondiente. En este caso, un usuario inicie una aplicación o un escritorio y cierra el explorador, continúa trabajando en la aplicación o el escritorio iniciados. Se agotó el tiempo de espera de la sesión de autenticación, autorización y auditoría, pero la conexión sigue activa. El número total de usuarios conectados se puede utilizar para identificar a los usuarios que siguen conectados.
- En HDX, la redirección óptima, la puerta de enlace de autenticación y la puerta de enlace ICA pueden estar en diferentes dispositivos. El total de usuarios conectados en este caso se puede utilizar para identificar el número de usuarios conectados en la puerta de enlace ICA.

Puntos a tener en cuenta:

- Los usuarios actuales superan el total de usuarios conectados cuando hay sesiones activas (aún no se ha agotado el tiempo de espera) pero no hay conexiones activas en estas sesiones. Por ejemplo, un usuario inició una aplicación o un escritorio y lo cerró inmediatamente, pero no cerró la sesión de autenticación, autorización y auditoría.
- El total de usuarios conectados supera a los usuarios actuales si se agota el tiempo de espera de las sesiones de autenticación, autorización y auditoría, pero las conexiones ICA siguen activas.
- En una configuración de VPN pura (no se trata de ICA), el número de usuarios actuales y el total de usuarios conectados son iguales.

Configurar los tipos de conexión en el servidor virtual

Al crear y configurar un servidor virtual, puede configurar las siguientes opciones de conexión:

- Conexiones con la aplicación Citrix Workspace solo a Citrix Virtual Apps and Desktops sin SmartAccess, análisis de puntos finales ni funciones de túnel de capa de red.
- Conexiones con el cliente Citrix Secure Access y SmartAccess, que permiten el uso de las funciones SmartAccess, de análisis de terminales y de tunelización de la capa de red.
- Conexiones con Secure Hub que establece una conexión Micro VPN desde dispositivos móviles a NetScaler Gateway.
- Conexiones paralelas realizadas a través del protocolo de sesión ICA por un usuario desde varios dispositivos. Las conexiones se migran a una sola sesión para evitar el uso de varias licencias universales.

Si quiere que los usuarios inicien sesión sin software de usuario, puede configurar una directiva de acceso sin cliente y vincularla al servidor virtual.

Para configurar conexiones Basic o SmartAccess en un servidor virtual

1. Vaya a **NetScaler Gateway** y, a continuación, haga **clic en Servidores**
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el servidor virtual.
4. En **Dirección IP** y **puerto**, escriba la dirección IP y el número de puerto del servidor virtual.
5. Lleve a cabo una de las siguientes acciones:
    - Para permitir únicamente conexiones ICA, haga clic en **Modo básico**.
    - Para permitir el inicio de sesión del usuario con Secure Hub, el cliente Citrix Secure Access y SmartAccess, haga clic en Modo **SmartAccess**.
    - Para permitir que SmartAccess administre las sesiones de proxy ICA para conexiones de varios usuarios, haga clic en **Migración de sesiones de proxy ICA**.

6. Configure los demás ajustes del servidor virtual, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Configurar una directiva de escucha para servidores virtuales comodín

Puede configurar los servidores virtuales de NetScaler Gateway para restringir la capacidad de un servidor virtual de escuchar en una VLAN específica. Puede crear un servidor virtual comodín con una directiva de escucha que lo restrinja al procesamiento del tráfico en la VLAN especificada.

Los parámetros de configuración son los siguientes:

Parámetro	Descripción
Nombre	Nombre del servidor virtual. El nombre es obligatorio y no se puede cambiar después de crear el servidor virtual. El nombre no puede superar los 127 caracteres y el primer carácter debe ser un número o una letra. También puede usar los siguientes caracteres: símbolo (@), guión bajo (_), guión (-), punto (.), dos puntos (:), signo de almohadilla (#) y un espacio.
IP	Dirección IP del servidor virtual. Para un servidor virtual comodín vinculado a la VLAN, el valor siempre es *.
Tipo	El comportamiento del servicio. Sus opciones son HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP y RTSP.
Puerto	Puerto en el que el servidor virtual escucha las conexiones de usuario. El número de puerto debe estar comprendido entre 0 y 65535. Para el servidor virtual comodín enlazado a una VLAN, el valor suele ser *.
Escucha Prioridad	La prioridad que se asigna a la directiva de escucha. La prioridad se evalúa en orden inverso; cuanto menor sea el número, mayor será la prioridad asignada a la directiva de escucha.

Parámetro	Descripción
Regla de directiva de escucha	Regla de directiva que se va a utilizar para identificar la VLAN a la que debe escuchar el servidor virtual. La regla es `CLIENT.VLAN.ID.EQ (<ipaddressat>)`. `<ipaddressat>` Sustitúyalo por el ID asignado a la VLAN.

Para crear un servidor virtual comodín con una directiva de escucha

1. En el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el servidor virtual.
4. En **Protocolo**, seleccione el protocolo.
5. En **Dirección IP**, escriba la dirección IP del servidor virtual.
6. En **Puerto**, escriba el puerto del servidor virtual.
7. En la ficha **Avanzadas**, en Directiva de escucha, en **Prioridad de escucha**, escriba la prioridad de la directiva de escucha.
8. Junto a Regla de directiva de escucha, haga clic en **Configurar**.
9. En el cuadro de diálogo **Crear expresión**, haga clic en **Agregar**, configure la expresión y, a continuación, haga clic en **Aceptar**.
10. Haga clic en **Create** y, luego, en **Close**.

Configuración de direcciones IP en NetScaler Gateway

January 26, 2024

Puede configurar direcciones IP para iniciar sesión en la utilidad de configuración y para las conexiones de usuario. NetScaler Gateway está configurado con una dirección IP predeterminada de 192.168.100.1 y una máscara de subred 255.255.0.0 para el acceso de administración. La dirección IP predeterminada se utiliza cuando no hay un valor configurado por el usuario para la dirección IP del sistema (NSIP).

- Dirección NSIP. Dirección IP de administración de NetScaler Gateway que se utiliza para todos los accesos relacionados con la administración al dispositivo. NetScaler Gateway también utiliza la dirección NSIP para la autenticación.

- Puerta de**enlace predeterminada**. Enrutador que reenvía el tráfico desde fuera de la red segura a NetScaler Gateway.
- **Dirección IP de subred (SNIP)**. Dirección IP que representa el dispositivo del usuario mediante la comunicación con un servidor de una red secundaria.

La dirección SNIP utiliza los puertos 1024 a 64000.

Cómo utiliza NetScaler Gateway las direcciones IP

NetScaler Gateway obtiene el tráfico de las direcciones IP en función de la función que se está produciendo. En la lista siguiente se describen varias funciones y la forma en que NetScaler Gateway utiliza las direcciones IP para cada una de ellas, como pauta general:

- **Autenticación.** La dirección IP que utiliza NetScaler Gateway depende del tipo de servidor de autenticación.
  - Servidores LDAP/RADIUS/TACACS. Si AAAD se comunica directamente con el servidor virtual de autenticación, se utiliza la dirección NSIP.
  - Si se utiliza un equilibrador de carga como proxy, el equilibrador de carga utiliza la dirección SNIP para la autenticación. AAAD utiliza la dirección NSIP para comunicarse con el equilibrador de carga. La dirección IP que utiliza NetScaler depende de la entidad que se comunica con el servidor virtual de autenticación.
  - Servidores SAML/OAUTH/WEBAUTH: Estos servidores se comunican mediante la dirección SNIP.
- **Transferencias de archivos desde la página principal.** NetScaler Gateway utiliza la dirección SNIP.
- **Consultas DNS y WINS.** NetScaler Gateway utiliza la dirección SNIP.
- **Tráfico de red a los recursos de la red segura.** NetScaler Gateway utiliza la dirección SNIP o la agrupación de IP, según la configuración de NetScaler Gateway.
- **Configuración del proxy ICA.** NetScaler Gateway utiliza la dirección SNIP.

Direcciones IP de subred

La dirección IP de subred permite al usuario conectarse a NetScaler Gateway desde un host externo que reside en otra subred. Al agregar una dirección IP de subred, se realiza una entrada de ruta correspondiente en la tabla de rutas. Solo se realiza una entrada por subred. La entrada de ruta corresponde a la primera dirección IP agregada en la subred.

A diferencia de la dirección IP del sistema y la dirección IP asignada, no es obligatorio especificar la dirección IP de subred durante la configuración inicial de NetScaler Gateway.

La dirección IP asignada y las direcciones IP de subred utilizan los puertos 1024 a 64000.

Para agregar una dirección IP de subred

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema\ > Red**y, a continuación, haga clic en **IP**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo Crear IP, en Dirección IP, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred.
5. En Tipo de IP, seleccione IP de subred, haga clic en **Cerrar y,** a continuación, haga clic en **Crear**.

Configurar IPv6 para conexiones de usuario

Puede configurar NetScaler Gateway para que escuche las conexiones de los usuarios mediante el Protocolo de Internet versión 6 (IPv6). Al configurar una de las siguientes opciones, puede activar la casilla de verificación IPv6 y, a continuación, introducir la dirección IPv6 en el cuadro de diálogo:

- Configuración global - Aplicaciones publicadas - ICA Proxy
- Autentificación global: RADIUS
- Autenticación global: LDAP
- Autenticación global - TACACS
- Perfil de sesión - Aplicaciones publicadas - ICA Proxy
- Servidores virtuales NetScaler Gateway
- Crear servidor de autenticación: RADIUS
- Crear servidor de autenticación: LDAP
- Crear servidor de autenticación - TACACS
- Crear servidor de auditoría
- Configuración de alta disponibilidad
- Enlazar o desvincular monitores de ruta para obtener alta disponibilidad
- Servidor virtual (equilibrio de carga)

Al configurar el servidor virtual NetScaler Gateway para que escuche en una dirección IPv6, los usuarios solo pueden conectarse con la aplicación Citrix Workspace. Las conexiones de usuario con el cliente Citrix Secure Access no se admiten con IPv6.

Puede utilizar las siguientes directrices para configurar IPv6 en NetScaler Gateway:

- Citrix Virtual Apps e Interfaz Web. Al configurar IPv6 para conexiones de usuario y si hay una dirección IP asignada que utiliza IPv6, los servidores de Citrix Virtual Apps e Interfaz Web también pueden usar IPv6. La Interfaz Web debe instalarse detrás de NetScaler Gateway. Cuando los usuarios se conectan a través de NetScaler Gateway, la dirección IPv6 se traduce a IPv4. Cuando vuelve la conexión, la dirección IPv4 se traduce a IPv6.
- Servidores virtuales. Puede configurar IPv6 para un servidor virtual cuando ejecuta el asistente de NetScaler Gateway. En el asistente de NetScaler Gateway de la página Servidores virtuales,

haga clic en IPv6 e introduzca la dirección IP. Solo puede utilizar la configuración de una dirección IPv6 para un servidor virtual mediante el asistente de NetScaler Gateway.
- Otros. Para configurar IPv6 para proxy ICA, autenticación, auditoría y alta disponibilidad, active la casilla de verificación IPv6 en el cuadro de diálogo y, a continuación, escriba la dirección IP.

Resolver servidores DNS ubicados en la red segura

January 26, 2024

Si su servidor DNS se encuentra en la red segura detrás de un firewall y el firewall bloquea el tráfico ICMP, no podrá probar las conexiones con el servidor porque el firewall bloquea la solicitud. Puede resolver este problema siguiendo los siguientes pasos:

- Creación de un servicio DNS con un monitor DNS personalizado que se resuelve en un nombre de dominio completo (FQDN) conocido.
- Creación de un servidor virtual DNS no direccionable directamente en NetScaler Gateway.
- Vincular el servicio al servidor virtual.

Nota:

- Configure un servidor virtual DNS y un servicio DNS solo si el servidor DNS se encuentra detrás de un firewall.
- Si instala una licencia de equilibrio de carga de NetScaler en el dispositivo, el nodo Servidores y servicios virtuales no aparece en el panel de navegación. Puede realizar este procedimiento expandiendo Equilibrio de carga y, a continuación, haciendo clic en Servidores virtuales.

Para configurar un servicio DNS y un monitor DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Servidores y servicios virtuales y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servicio.
4. En Protocolo, selecciona DNS.
5. En Dirección IP, escriba la dirección IP del servidor DNS.
6. En Puerto, escriba el número de puerto.
7. En la ficha Servicios, haga clic en Agregar.
8. En la ficha Monitores, en Disponible, seleccione DNS, haga clic en Agregar, en Crear y, a continuación, en Cerrar.
9. En el cuadro de diálogo Crear servidor virtual (equilibrio de carga), haga clic en Crear y, a continuación, en Cerrar.

A continuación, cree el servidor virtual DNS mediante el procedimiento Para configurar un servidor virtual DNS y, a continuación, enlazar el servicio DNS al servidor virtual.

Para enlazar un servicio DNS a un servidor virtual DNS

1. En el cuadro de diálogo Configurar servicio virtual (equilibrio de carga), en la ficha Servicios, haga clic en Agregar, seleccione el servicio DNS, haga clic en Crear y, a continuación, haga clic en Cerrar.

Configurar servidores virtuales DNS

January 26, 2024

Para configurar un servidor virtual DNS, especifique un nombre y una dirección IP. Al igual que el servidor virtual de NetScaler Gateway, debe asignar una dirección IP al servidor virtual DNS. Sin embargo, esta dirección IP debe estar en el lado interno de la red de destino para que los dispositivos de usuario resuelvan todas las direcciones internas. Además, especifique el puerto DNS.

Nota: Si instala una licencia de equilibrio de carga de NetScaler en el dispositivo, el nodo Servidores y servicios
virtuales no aparece en el panel de navegación. Puede configurar esta función mediante el servidor virtual de equilibrio de carga. Para obtener más información, consulte la documentación de NetScaler en la documentación del producto NetScaler.

Para configurar un servidor virtual DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Servidores y servicios virtuales y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el servidor virtual.
4. En Dirección IP, escriba la dirección IP del servidor DNS.
5. En Puerto, escriba el puerto en el que escucha el servidor DNS.
6. En Protocolo, seleccione DNS y, a continuación, haga clic en Crear.

Por último, asocie el servidor virtual DNS con NetScaler Gateway mediante uno de los dos métodos siguientes, según las necesidades de la implementación:

- Enlazar el servidor globalmente a NetScaler Gateway.
- Enlazar el servidor virtual DNS por servidor virtual.

Si implementa el servidor virtual DNS de forma global, todos los usuarios tienen acceso a él. A continuación, puede restringir a los usuarios vinculando el servidor virtual DNS al servidor virtual.

Configurar proveedores de servicios de nombres

March 27, 2024

NetScaler Gateway utiliza proveedores de servicios de nombres para convertir direcciones web en direcciones IP.

Al ejecutar el asistente de NetScaler Gateway, puede configurar un servidor DNS o un servidor WINS. Puede utilizar la utilidad de configuración para configurar también otros servidores DNS o WINS.

Para agregar un servidor DNS a NetScaler Gateway

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Configuración de red, haga clic en Agregar.
4. En el cuadro de diálogo Insertar servidor de nombres, en Dirección IP, escriba la dirección IP del servidor DNS, haga clic en Crear y, a continuación, haga clic en Cerrar.
5. Haga clic en Aceptar en la utilidad de configuración.

Para agregar un servidor WINS a NetScaler Gateway

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Configuración de red, en IP del servidor WINS, escriba la dirección IP del servidor WINS y, a continuación, haga clic en Aceptar.

A continuación, especifique el nombre del servidor virtual DNS y la dirección IP. Al igual que el servidor virtual de NetScaler Gateway, se debe asignar una dirección IP al servidor virtual. Sin embargo, esta dirección IP debe estar en el lado interno de la red de destino para que los dispositivos de usuario resuelvan correctamente todas las direcciones internas. También debe especificar el puerto DNS.

Si configura un servidor DNS y un servidor WINS para la resolución de nombres, puede utilizar el asistente de NetScaler Gateway para seleccionar qué servidor realiza primero la búsqueda de nombres.

Para especificar la prioridad de búsqueda de nombres

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente de NetScaler Gateway .
3. Haga clic en Siguiente para aceptar la configuración actual hasta que acceda a la página Proveedores de servicios de nombres.
4. En Prioridad de búsqueda de nombres, seleccione WINS o DNS y, a continuación, continúe hasta el final del asistente.

Configurar conexiones iniciadas por el servidor

March 27, 2024

Para cada usuario que inició sesión en NetScaler Gateway con direcciones IP habilitadas, el sufijo DNS se anexa al nombre de usuario y se agrega un registro de dirección DNS a la caché DNS del dispositivo. Esta técnica ayuda a proporcionar a los usuarios un nombre DNS en lugar de las direcciones IP de los usuarios.

Cuando se asigna una dirección IP a la sesión de un usuario, es posible conectarse al dispositivo del usuario desde la red interna. Por ejemplo, los usuarios que se conectan con el cliente de escritorio remoto o de computación en red virtual (VNC) pueden acceder al dispositivo de usuario para diagnosticar una aplicación problemática. También es posible que dos usuarios de NetScaler Gateway con direcciones IP de red internas que hayan iniciado sesión de forma remota se comuniquen entre sí a través de NetScaler Gateway. Permitir el descubrimiento de las direcciones IP de la red interna de los usuarios que han iniciado sesión en el dispositivo ayuda a esta comunicación.

Un usuario remoto puede utilizar el siguiente comando ping para descubrir la dirección IP de la red interna de un usuario que puede iniciar sesión en NetScaler Gateway:

```
ping \<username.domainname\>
```

Un servidor puede iniciar una conexión con un dispositivo de usuario de las siguientes formas:

- Conexiones TCP o UDP. Las conexiones pueden originarse en un sistema externo de la red interna o en otro equipo que haya iniciado sesión en NetScaler Gateway. La dirección IP de red interna asignada a cada dispositivo de usuario que ha iniciado sesión en NetScaler Gateway se utiliza para estas conexiones. Se describen los distintos tipos de conexiones iniciadas por el servidor que admite NetScaler Gateway.
  Para las conexiones iniciadas por el servidor TCP o UDP, el servidor tiene conocimiento previo de la dirección IP y el puerto del dispositivo del usuario y establece una conexión con él. NetScaler Gateway intercepta esta conexión.

A continuación, el dispositivo del usuario establece una conexión inicial con el servidor y el servidor se conecta al dispositivo de usuario en un puerto conocido o derivado del primer puerto configurado.

En este caso, el dispositivo del usuario establece una conexión inicial con el servidor y, a continuación, intercambia puertos y direcciones IP con el servidor mediante un protocolo específico de la aplicación en el que se incrusta esta información. Esto permite que NetScaler Gateway admita aplicaciones, como conexiones FTP activas.

- Comando Port. Se utiliza en un FTP activo y en determinados protocolos de voz sobre IP.
- Conexiones entre plug-ins. NetScaler Gateway admite conexiones entre complementos mediante las direcciones IP de la red interna.

  Con este tipo de conexión, dos dispositivos de usuario de NetScaler Gateway que utilizan el mismo NetScaler Gateway pueden iniciar conexiones entre sí. Un ejemplo de este tipo es el uso de aplicaciones de mensajería instantánea, como Office Communicator o Yahoo! Mensajero.

Si un usuario cierra la sesión de NetScaler Gateway y la solicitud de cierre de sesión no llega al dispositivo, el usuario puede volver a iniciar sesión con cualquier dispositivo y reemplazar la sesión anterior por una nueva. Esta función puede ser beneficiosa en implementaciones en las que se asigna una dirección IP por usuario.

Cuando un usuario inicia sesión en NetScaler Gateway por primera vez, se crea una sesión y se asigna una dirección IP al usuario. Si el usuario cierra la sesión pero se pierde la solicitud de cierre de sesión o el dispositivo del usuario no realiza un cierre de sesión limpio, la sesión se mantiene en el sistema. Si el usuario intenta iniciar sesión de nuevo desde el mismo dispositivo u otro dispositivo, tras una autenticación correcta, aparece un cuadro de diálogo de inicio de sesión de transferencia. Si el usuario decide transferir el inicio de sesión, la sesión anterior de NetScaler Gateway se cierra y se crea una nueva sesión. La transferencia de inicio de sesión está activa solo dos minutos después del cierre de sesión, y si se intenta iniciar sesión desde varios dispositivos simultáneamente, el último intento de inicio de sesión reemplaza la sesión original.

Configurar el rango de puertos privados para las conexiones iniciadas por el servidor

A partir de la versión 23.10.1.7 del cliente Citrix Secure Access, puede configurar un puerto privado que vaya del 49152 al 64535 para las conexiones iniciadas por el servidor (SIC). La configuración de puertos privados evita los conflictos que pueden surgir al utilizar los puertos para crear sockets entre el cliente Citrix Secure Access y las aplicaciones de terceros en las máquinas cliente. Esto solo se aplica si el controlador del WFP está en uso.

Puede configurar los puertos privados mediante el `SicBeginPort`registro de VPN de Windows. Como alternativa, puede configurar el rango de puertos privados mediante un archivo JSON de personalización del complemento VPN en NetScaler.

Si un servidor inicia una conexión, el cliente Citrix Secure Access utiliza los primeros 1000 puertos, empezando por `SicBeginPort`el Registro de VPN de Windows, para crear los sockets. Si el registro está configurado en un equipo cliente, la configuración del registro tiene prioridad sobre la configuración JSON de NetScaler.

El siguiente es un ejemplo de la configuración JSON del complemento VPN en NetScaler:

```
root@ADC# cat /var/netscaler/gui/vpn/pluginCustomization.json

{
 "SicBeginPort" : 51000 }

<!--NeedCopy-->
```

Para obtener más información sobre la configuración del registro, consulte Claves de registro del cliente VPN de Windows de NetScaler Gateway.

> **Nota:**
>
> El rango de puertos predeterminado que se usa para crear sockets es 62500—63500.

Configurar la redirección en NetScaler Gateway

March 27, 2024

Para proporcionar acceso a los recursos de la red interna, NetScaler Gateway enruta los datos a sus redes internas seguras. De forma predeterminada, NetScaler Gateway utiliza una ruta estática.

Las redes a las que NetScaler Gateway puede redirigir los datos se determinan por la forma en que se configura la tabla de redirección de NetScaler Gateway y la puerta de enlace predeterminada especificada para NetScaler Gateway.

La tabla de redirección de NetScaler Gateway debe contener las rutas necesarias para redirigir los datos a cualquier recurso de red interna al que un usuario necesite acceder.

NetScaler Gateway admite los siguientes protocolos de redirección:

- Protocolo de información de redirección (RIP v1 y v2)
- Abrir primero el trayecto más corto (OSPF)
- Protocolo de puerta de enlace fronteriza (BGF)

Configurar una ruta estática

Al configurar la comunicación con otro host o red, debe configurar una ruta estática desde NetScaler Gateway al nuevo destino si no utiliza la redirección dinámica.

Para configurar una ruta estática

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Red > Avanzado** y, a continuación, haga clic en **Rutas**.
2. En el panel de detalles, en la ficha Básico, haga clic en **Agregar**.
3. Configure los ajustes de la ruta y, a continuación, haga clic en **Crear**.

Para probar una ruta estática

1. En la utilidad de configuración, en el panel de navegación, expanda **Sistema y,** a continuación, haga clic en **Diagnóstico**.
2. En el panel de detalles, en Utilidades, haga clic en **Ping**.
3. En Parámetros, en Nombre de host, escriba el nombre del dispositivo.
4. En Avanzado, en Dirección IP de origen, escriba la dirección IP del dispositivo y, a continuación, haga clic en **Ejecutar**.

   Si se comunica correctamente con el otro dispositivo, los mensajes indican que se transmitieron y recibieron el mismo número de paquetes y que se perdieron cero paquetes.

   Si no se comunica con el otro dispositivo, los mensajes de estado indican que se han recibido cero paquetes y se han perdido todos los paquetes. Para corregir esta falta de comunicación, repita el procedimiento para agregar una ruta estática.

Para detener la prueba, en el cuadro de diálogo **Ping**, haga clic en **Detener y,** a continuación, en **Cerrar**.

Configurar la negociación automática

March 27, 2024

De forma predeterminada, el dispositivo está configurado para utilizar la negociación automática, en la que NetScaler Gateway transmite el tráfico de red en ambas direcciones simultáneamente y determina la velocidad del adaptador adecuada. Si deja la configuración predeterminada en Negociación automática, NetScaler Gateway utiliza la operación de dúplex completo, en la que el adaptador de red puede enviar datos en ambas direcciones simultáneamente.

Si inhabilita la negociación automática, NetScaler Gateway utiliza la operación semidúplex, en la que el adaptador puede enviar datos en ambas direcciones entre dos nodos, pero el adaptador solo puede usar una dirección u otra a la vez.

Para la primera instalación, Citrix recomienda configurar NetScaler Gateway para que utilice la negociación automática en los puertos conectados al dispositivo. Después de iniciar sesión inicialmente y configurar NetScaler Gateway, puede inhabilitar la negociación automática. No se puede configurar la negociación automática de forma global. Debe habilitar o inhabilitar la configuración para cada interfaz.

Para habilitar o inhabilitar la negociación automática

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema\ > Red y, a continuación,** haga clic en **Interfaces**.
2. En el panel de detalles, seleccione la interfaz y, a continuación, haga clic en **Abrir**.
3. Realice una de las siguientes acciones en el cuadro de diálogo **Configurar interfaz**:
    - Para habilitar la negociación automática, haga clic en **Sí** junto a Negociación automática y, a continuación, haga clic en **Aceptar**.
    - Para inhabilitar la negociación automática, haga clic en **No** junto a Negociación automática y, a continuación, haga clic en **Aceptar**.

Configurar el nombre de host y el FQDN en NetScaler Gateway

January 26, 2024

El nombre de host es el nombre del dispositivo NetScaler Gateway asociado al archivo de licencia. El nombre de host es exclusivo del dispositivo y se utiliza al descargar la licencia Universal. Defina el nombre de host al ejecutar el Asistente de configuración para configurar NetScaler Gateway por primera vez.

El nombre de dominio completo (FQDN) se incluye en el certificado firmado vinculado a un servidor virtual. No se configura el FQDN en NetScaler Gateway. Un dispositivo puede tener un FQDN único asignado a cada servidor virtual configurado en NetScaler Gateway mediante certificados.

Puede encontrar el FQDN de un certificado consultando los detalles del certificado. El FQDN se encuentra en el campo de asunto del certificado.

Para ver el FQDN de un certificado

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **SSL y, a continuación,** haga clic en **Certificados**.
2. En el panel de detalles, seleccione un certificado, haga clic en **Acción y,** a continuación, haga clic en **Detalles**.

3. En el cuadro de diálogo Detalles del certificado, haga clic en **Asunto**. El FQDN del certificado aparece en la lista.

Directivas y perfiles en NetScaler Gateway

March 27, 2024

Las directivas y los perfiles de NetScaler Gateway permiten administrar e implementar los valores de configuración en situaciones o condiciones específicas. Una directiva individual establece o define los valores de configuración que entran en vigor cuando se cumple un conjunto de condiciones especificado. Cada directiva tiene un nombre único y puede tener un perfil vinculado a la directiva.

Cómo funcionan las directivas

Una directiva consiste en una condición booleana y un conjunto de ajustes denominados perfil. La condición se evalúa en tiempo de ejecución para determinar si se debe aplicar la directiva.

Un perfil es un conjunto de configuraciones que utilizan parámetros específicos. El perfil puede tener cualquier nombre y puede reutilizarlo en más de una directiva. Puede configurar varias opciones dentro del perfil, pero solo puede incluir un perfil por directiva.

Puede enlazar directivas, con las condiciones y los perfiles configurados, a servidores virtuales, grupos, usuarios o de forma global. Las directivas se denominan por el tipo de configuración que controlan. Por ejemplo, en una directiva de sesión, puede controlar cómo inician sesión los usuarios y el número de veces que los usuarios pueden permanecer conectados.

Si utiliza NetScaler Gateway con Citrix Virtual Apps, los nombres de directiva de NetScaler Gateway se envían a Citrix Virtual Apps como filtros. Al configurar NetScaler Gateway para que sea compatible con Citrix Virtual Apps y SmartAccess, configure las siguientes opciones en Citrix Virtual Apps:

- Nombre del servidor virtual configurado en el dispositivo. El nombre se envía a Citrix Virtual Apps como nombre de comunidad de NetScaler Gateway.
- Los nombres de las directivas de sesión o autenticación previa se envían como nombres de filtro.

Para obtener más información sobre cómo configurar NetScaler Gateway para que sea compatible con Citrix Endpoint Management, consulteConfiguración de las opciones del entorno de Citrix Endpoint Management.

Para obtener más información sobre cómo configurar NetScaler Gateway para que sea compatible con Citrix Virtual Apps and Desktops, consulteAcceso a recursos de Citrix Virtual Apps y Citrix Virtual Desktops con la Interfaz WebeIntegración con Citrix Endpoint Management o StoreFront.

Para obtener más información sobre las directivas de autenticación previa, consulte Configuración de directivas de endpoint.

Directivas condicionales

Al configurar directivas, puede utilizar cualquier expresión booleana para expresar la condición de cuándo se aplica la directiva. Al configurar directivas condicionales, puede utilizar cualquiera de las expresiones del sistema disponibles, como las siguientes:

- Cadenas de seguridad del cliente
- Información de red
- Encabezados HTTP y cookies
- Hora del día
- Valores de certificados de cliente

También puede crear directivas para aplicarlas solo cuando el dispositivo de usuario cumpla criterios específicos, como una directiva de sesión para SmartAccess.

Otro ejemplo de configuración de una directiva condicional es la variación de la directiva de autenticación para los usuarios. Por ejemplo, puede exigir que los usuarios que se conectan al cliente Citrix Secure Access desde fuera de la red interna, como desde el ordenador de su casa o mediante Micro VPN desde un dispositivo móvil, se autentiquen mediante LDAP y que los usuarios que se conecten a través de la WAN se autentiquen mediante RADIUS.

Nota : No puede usar condiciones de política basadas en los resultados del análisis de terminales si la regla de política está configurada como parte de la configuración de seguridad de un perfil de sesión.

Prioridades de las directivas

Las directivas se priorizan y evalúan en el orden en que está vinculada la directiva.

Los dos métodos siguientes determinan la prioridad de la directiva:

- Nivel al que está vinculada la directiva: globalmente, servidor virtual, grupo o usuario. Los niveles de directivas se clasifican del más alto al más bajo de la siguiente manera:
  - Usuario (prioridad máxima)
  - Grupo
  - Servidor virtual
  - Global (prioridad más baja)
- La prioridad numérica tiene prioridad independientemente del nivel al que esté vinculada la directiva. Si una directiva vinculada globalmente tiene un número de prioridad de uno y otra

directiva vinculada a un usuario tiene un número de prioridad de dos, la directiva global tiene prioridad. Un número de prioridad más bajo otorga a la directiva una mayor prioridad.

Creación de directivas en NetScaler Gateway

Puede utilizar la utilidad de configuración para crear directivas. Después de crear una directiva, la vincula al nivel adecuado: usuario, grupo, servidor virtual o global. Cuando vincula una directiva a uno de estos niveles, los usuarios reciben la configuración dentro del perfil si se cumplen las condiciones de la directiva. Cada directiva y perfil tiene un nombre único.

Si tiene Citrix Endpoint Management o StoreFront como parte de la implementación, puede utilizar el Asistente de configuración rápida para configurar los ajustes de esta implementación. Para obtener más información sobre el asistente, consulte Configuración de los ajustes con el Asistente de configuración rápida.

Configurar expresiones del sistema

March 27, 2024

Una expresión del sistema especifica las condiciones en las que se aplica la directiva. Por ejemplo, las expresiones de una directiva de autenticación previa se aplican mientras un usuario inicia sesión. Las expresiones de una directiva de sesión se evalúan y aplican después de autenticar al usuario e iniciar sesión en NetScaler Gateway.

Las expresiones de NetScaler Gateway incluyen:

- Expresiones generales que limitan los objetos que los usuarios pueden usar al establecer una conexión con NetScaler Gateway. Por ejemplo, consulte:
  - Directivas de sesión
- Expresiones de seguridad de cliente que definen el software, los archivos, los procesos o los valores de registro que deben instalarse y ejecutarse en el dispositivo del usuario. Por ejemplo, consulte:
  - Directivas de dispositivos de punto final
- Expresiones basadas en la red que restringen el acceso en función de la configuración de la red. Por ejemplo, consulte:
  - Directivas de tráfico
  - Directivas de autorización

NetScaler Gateway también se puede utilizar como dispositivo NetScaler. Algunas expresiones del dispositivo son más aplicables a NetScaler. Las expresiones generales y basadas en red se utilizan habitualmente con NetScaler y no suelen utilizarse con NetScaler Gateway. Las expresiones de seguridad del cliente se utilizan en NetScaler Gateway para determinar que los elementos correctos están instalados en el dispositivo del usuario.

Configuración de expresiones de seguridad de clientes

Las expresiones son un componente de una directiva. Una expresión representa una condición única que se evalúa con respecto a una solicitud o una respuesta. Puede crear una cadena de seguridad de expresión sencilla para comprobar si hay condiciones, tales como:

- Sistema operativo del dispositivo de usuario, incluidos los service packs
- Definiciones de virus y versión del software antivirus
- Archivos
- Procesos
- Valores de registro
- Certificados de usuario

Administración de certificados en NetScaler Gateway

January 26, 2024

En NetScaler Gateway, utiliza certificados para crear conexiones seguras y autenticar usuarios.

Para establecer una conexión segura, se requiere un certificado de servidor en un extremo de la conexión. Se requiere un certificado raíz de la entidad emisora de certificados (CA) que emitió el certificado del servidor en el otro extremo de la conexión.

- Certificado de servidor. Un certificado de servidor certifica la identidad del servidor. NetScaler Gateway requiere este tipo de certificado digital.
- Certificado raíz. Un certificado raíz identifica a la CA que firmó el certificado de servidor. El certificado raíz pertenece a la entidad emisora de certificados. Un dispositivo de usuario requiere este tipo de certificado digital para verificar el certificado del servidor.

Al establecer una conexión segura con un explorador web en el dispositivo del usuario, el servidor envía su certificado al dispositivo.

Cuando el dispositivo de usuario recibe un certificado de servidor, el explorador web, como Internet Explorer, comprueba qué CA emitió el certificado y si el dispositivo del usuario confía en la entidad emisora de certificados. Si la entidad emisora de certificados no es de confianza o si se trata de un

certificado de prueba, el explorador web solicita al usuario que acepte o rechace el certificado (aceptando o rechazando efectivamente la capacidad de acceder al sitio).

NetScaler Gateway admite los tres tipos de certificados siguientes:

- Certificado de prueba enlazado a un servidor virtual y que también se puede utilizar para conexiones a una comunidad de servidores. NetScaler Gateway incluye un certificado de prueba preinstalado.
- Certificado en formato PEM o DER firmado por una entidad emisora de certificados y emparejado con una clave privada.
- Certificado en formato PKCS #12 que se utiliza para almacenar o transportar el certificado y la clave privada. El certificado PKCS #12 se exporta normalmente de un certificado de Windows existente como archivo PFX y, a continuación, se instala en NetScaler Gateway.

Citrix recomienda utilizar un certificado firmado por una entidad emisora de certificados de confianza, como Thawte o Verisign.

Crear una solicitud de firma de certificado

March 27, 2024

Para proporcionar comunicaciones seguras mediante SSL o TLS, se requiere un certificado de servidor en NetScaler Gateway. Antes de cargar un certificado en NetScaler Gateway, debe generar una solicitud de firma de certificado (CSR) y una clave privada. Utilice la solicitud de creación de certificado incluida en el asistente de NetScaler Gateway o la utilidad de configuración para crear la CSR. La solicitud de creación de certificado crea un archivo.csr que se envía por correo electrónico a la entidad de certificación (CA) para que lo firme y una clave privada que permanece en el dispositivo. La CA firma el certificado y se lo devuelve a la dirección de correo electrónico que proporcionó. Cuando reciba el certificado firmado, podrá instalarlo en NetScaler Gateway. Cuando reciba el certificado de la entidad emisora de certificados, empareja el certificado con la clave privada.

Importante: Cuando utilice el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y esperar a que la CA le envíe el certificado firmado. Cuando reciba el certificado, puede volver a ejecutar el asistente de NetScaler Gateway para crear la configuración e instalar el certificado. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

Crear una CSR mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.

2. En el panel de detalles, en Introducción, haga clic en el asistente de **NetScaler Gateway** .
3. Siga las instrucciones del asistente hasta llegar a la página Especificar un certificado de servidor.
4. Haga clic en **Crear una solicitud de firma de certificado** y complete los campos.
   Nota: El nombre de dominio completo (FQDN) no tiene por qué ser el mismo que el nombre de host de NetScaler Gateway. El FQDN se utiliza para el inicio de sesión del usuario.
5. Haga clic en **Crear** para guardar el certificado en el equipo y, a continuación, haga clic en **Cerrar**.
6. Salga del asistente de NetScaler Gateway sin guardar la configuración.

Crear una CSR mediante la GUI de NetScaler

También puede utilizar la GUI de NetScaler para crear una CSR sin ejecutar el asistente de NetScaler Gateway.

1. Vaya a **Administración de tráfico** > **SSL > Archivos SSL** y seleccione **Crear solicitud de firma de certificado (CSR)**.
2. Complete la configuración del certificado y, a continuación, haga clic en **Crear**.

Después de crear el certificado y la clave privada, envíe el certificado por correo electrónico a la CA, como Thawte o Verisign.

Para obtener información detallada sobre el procedimiento, consulte Crear una solicitud de firma de certificado.

Instalar el certificado firmado en NetScaler Gateway

Cuando reciba el certificado firmado de la entidad emisora de certificados (CA), emparéjelo con la clave privada del dispositivo y, a continuación, instale el certificado en NetScaler Gateway.

Empareja el certificado firmado con una clave privada mediante la interfaz gráfica de usuario

1. Copie el certificado en NetScaler Gateway en la carpeta nsconfig/ssl mediante un programa Secure Shell (SSH) como WinSCP.
2. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **SSL > Certificados**.
3. En la página **Certificado SSL**, haga clic en **Comenzar**.
4. En el panel de detalles, haga clic en **Instalar**.
5. En **Nombre del par de claves de certificado**, escriba el nombre del certificado.
6. En **Nombre de archivo de certificado**, haga clic **en Equipo**.
7. Vaya al certificado, haga clic en **Seleccionar** y, a continuación, en **Abrir**.

8. En **Nombre de archivo clave**, haga clic en **Equipo**. El nombre de la clave privada es el mismo que el de la solicitud de firma de certificado (CSR). La clave privada se encuentra en NetScaler Gateway en el directorio\ nsconfig\ ssl.
9. Elija la clave privada y, a continuación, haga clic en **Abrir**.
10. Si el certificado tiene formato PEM, en **Contraseña**, escriba la contraseña de la clave privada.
11. Si quiere configurar la notificación para cuándo caduca el certificado, seleccione **Notificar cuando caduque**.
12. En **Período de notificación**, escriba el número de días, haga clic en **Crear** y, a continuación, en **Cerrar**.

Enlazar el certificado y la clave privada a un servidor virtual mediante la interfaz gráfica de usuario

Después de crear y vincular un par de certificados y claves privadas, enlaza a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Certificados, en **Disponible**, seleccione un certificado, haga clic en **Agregar** y, a continuación, en **Aceptar**.

Enlazar el certificado y la clave privada a un servidor virtual mediante la CLI

En la línea de comandos, escriba;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
    ocspCheck Mandatory
<!--NeedCopy-->
```

Nota: OscpCheck es opcional si la comprobación OCSP no es necesaria para el certificado del dispositivo.

Desvincular certificados de prueba del servidor virtual mediante la interfaz gráfica de usuario

Después de instalar el certificado firmado, desvincule todos los certificados de prueba vinculados al servidor virtual. Puede desvincular certificados de prueba mediante la utilidad de configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Certificados, en **Configurado**, seleccione el certificado de prueba y, a continuación, haga clic en **Quitar**.

Configurar certificados intermedios

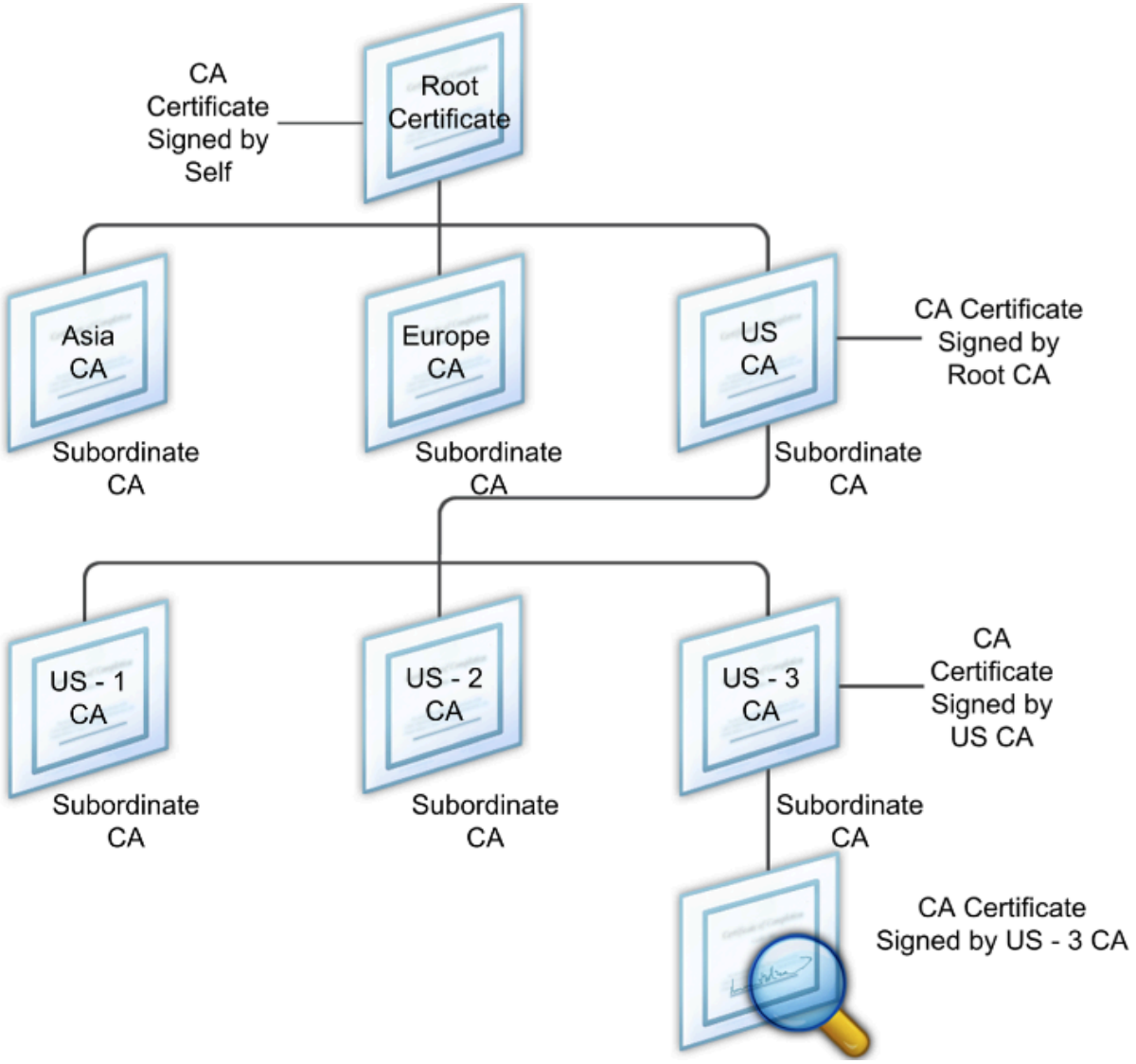
January 26, 2024

Un certificado intermedio es un certificado que va entre NetScaler Gateway (el certificado del servidor) y un certificado raíz (instalado en el dispositivo del usuario). Un certificado intermedio forma parte de una cadena.

Algunas organizaciones delegan la responsabilidad de emitir certificados para resolver el problema de la separación geográfica entre las unidades organizativas o para aplicar directivas de emisión diferentes a distintas secciones de la organización.

La responsabilidad de la emisión de certificados se puede delegar mediante la configuración de entidades de certificación (CA) subordinadas. Las entidades emisoras de certificados pueden firmar sus propios certificados (es decir, están autofirmados) o pueden firmarlos otra entidad emisora de certificados. El estándar X.509 incluye un modelo para configurar una jerarquía de CA. En este modelo, como se muestra en la siguiente ilustración, la CA raíz se encuentra en la parte superior de la jerarquía y es un certificado autofirmado por la entidad emisora de certificados. Las entidades emisoras de certificados que están directamente subordinadas a la entidad emisora de certificados raíz tienen certificados de CA firmados por la entidad emisora de certificados raíz. Las entidades emisoras de certificados subordinadas de la jerarquía tienen sus certificados de CA firmados por las entidades emisoras de certificados subordinadas.

Figura 1. El modelo X.509 muestra la estructura jerárquica de una cadena de certificados digitales típica



Si un certificado de servidor está firmado por una CA con un certificado autofirmado, la cadena de certificados se compone exactamente de dos certificados: el certificado de entidad final y la entidad emisora de certificados raíz. Si un certificado de usuario o servidor está firmado por una entidad emisora de certificados intermedia, la cadena de certificados es más larga.

En la siguiente ilustración se muestra que los dos primeros elementos son el certificado de entidad final (en este caso, gwy01.company.com) y el certificado de la entidad emisora de certificados intermedia, en ese orden. El certificado de la entidad emisora de certificados intermedia va seguido del certificado de su entidad emisora de certificados. Esta lista continúa hasta que el último certificado de la lista corresponde a una entidad emisora de certificados raíz. Cada certificado de la cadena da fe de la identidad del certificado anterior.

Figura 2. Una cadena de certificados digitales típica

Instalar un certificado intermedio

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, haga clic en Instalar.
3. En Nombre del par de claves de certificado, escriba el nombre del certificado.
4. En Detalles, en Nombre de archivo de certificado, haga clic en Examinar (dispositivo) y, en la lista, seleccione Local o Equipo.
5. Vaya a el certificado en su equipo (local) o en NetScaler Gateway (dispositivo).
6. En Formato de certificado, seleccione PEM.
7. Haga clic en Instalar y, a continuación, en Cerrar.

Al instalar un certificado intermedio en NetScaler Gateway, no es necesario especificar la clave privada ni la contraseña.

Una vez instalado el certificado en el dispositivo, el certificado debe vincularse al certificado del servidor.

Vincular un certificado intermedio a un certificado de servidor

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, seleccione el certificado de servidor y, a continuación, en Acción, haga clic en Vincular.
3. Junto a Nombre del certificado de CA, seleccione el certificado intermedio de la lista y, a continuación, haga clic en Aceptar.

Usar certificados de dispositivo para la autenticación

January 26, 2024

NetScaler Gateway admite la comprobación de certificados de dispositivo que permite vincular la identidad del dispositivo a la clave privada de un certificado. La comprobación del certificado del dispositivo se puede configurar como parte de las directivas clásicas o avanzadas de Endpoint Analysis (EPA). En las directivas clásicas de EPA, el certificado de dispositivo solo se puede configurar para la EPA de autenticación previa.

NetScaler Gateway verifica el certificado del dispositivo antes de que se ejecute el análisis de endpoint o antes de que aparezca la página de inicio de sesión. Si configura el análisis de endpoints, el análisis de endpoints se ejecuta para verificar el dispositivo del usuario. Cuando el dispositivo pasa el análisis y después de que NetScaler Gateway verifica el certificado del dispositivo, los usuarios pueden iniciar sesión en NetScaler Gateway.

> **Importante:**
>
> - De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo.
> - Para agregar una comprobación de certificado de dispositivo para usuarios que no son administradores, debe instalar el complemento VPN. La versión del plug-in VPN debe ser la misma que el plug-in de la EPA del dispositivo.
> - Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado de dispositivo.
> - Si instala dos o más certificados de dispositivo en NetScaler Gateway, los usuarios deben seleccionar el certificado correcto cuando empiecen a iniciar sesión en NetScaler Gateway o antes de que se ejecute el análisis de endpoint.
> - Al crear el certificado de dispositivo, debe ser un certificado X.509.
> - Si tiene un certificado de dispositivo emitido por una CA intermedia, los certificados de CA intermedia y raíz deben estar vinculados.
> - El cliente EPA necesita que el usuario tenga derechos de administrador local para poder acceder al almacén de certificados de la máquina. Esto rara vez ocurre, por lo que una solución alternativa es instalar el complemento completo de NetScaler Gateway que puede acceder al almacén local.

Para obtener más información sobre cómo crear certificados de dispositivo, consulte lo siguiente:

- Servicio de inscripción de dispositivos de red (NDES) en los Servicios de certificados de Active Directory (AD CS) en el sitio web de Microsoft.
- Cómo solicitar un certificado a una entidad emisora de certificados de Microsoft mediante DCE/RPC y la carga útil del perfil de certificados de Active Directory en el sitio web de soporte técnico de Apple.
- Emisión de certificados iPad o iPhone en el blog de soporte técnico de Microsoft Pregunte al equipo de servicios de directorio.
- Configuración del servicio de inscripción de dispositivos de red en el sitio web de TI Pro de

Windows.

- Ejemplo paso a paso de implementación de certificados PKI para Configuration Manager: ¿Entidad de certificación de Windows Server 2008? RedirectedFrom=MSDN) en el sitio web de Microsoft System Center.

Pasos para configurar certificados de dispositivo

Para configurar un certificado de dispositivo, debe completar los pasos siguientes:

- Instale el certificado de entidad emisora de certificados del dispositivo en NetScaler Gateway. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Enlace el certificado de entidad emisora de certificados del dispositivo al servidor virtual de NetScaler Gateway y habilite la comprobación de OCSP. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Cree y vincule OCSP (respondedor) en el certificado de entidad emisora de certificados del dispositivo. Para obtener más información, consulte Supervisar el estado de los certificados con OCSP.

Habilite la comprobación de certificados de dispositivo en el servidor virtual y agregue el certificado de entidad emisora de certificados de dispositivo a la lista de comprobación de certificados de dispositivo. Para obtener más información, consulte Habilitar la comprobación de certificados de dispositivo en un servidor virtual para la directiva clásica de EPA.

Complete la configuración del cliente y la verificación del certificado de dispositivo en la máquina Windows. Para obtener más información, consulte Verificación del certificado de dispositivo en un equipo Windows.

> **Nota:**
>
> Todos los clientes destinados a aprovechar la comprobación EPA del certificado de dispositivo deben tener el certificado de dispositivo instalado en el almacén de certificados del sistema de la máquina.

Habilitar la comprobación de certificados de dispositivo en un servidor virtual para la directiva clásica de EPA

Después de crear el certificado de dispositivo, instale el certificado en NetScaler Gateway mediante el procedimiento de importación e instalación de un certificado existente en NetScaler Gateway.

1. En la pestaña Configuración, vaya a **NetScaler Gateway > Servidores virtuales**.

2. En la página **Servidores virtuales de NetScaler Gateway**, seleccione un servidor virtual existente y haga clic en **Editar**.
3. En la página **Servidores virtuales VPN** , en la sección **Configuración básica** , haga clic en **Editar** .
4. Desactive la casilla **Habilitar autenticación** para inhabilitar la autenticación.
5. Seleccione la casilla **Habilitar certificado de dispositivo** para habilitar el certificado de dispositivo
6. Haga clic en **Agregar** para agregar a la lista el nombre del certificado de entidad emisora de certificados de dispositivo disponible.
7. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **CA para certificado de dispositivo**, haga clic en **Agregar**, seleccione el certificado y, a continuación, haga clic en **+**.

> **Nota:**
>
> Para obtener información sobre cómo habilitar y vincular certificados de dispositivo en un servidor virtual para directivas EPA avanzadas, consulte Certificado de dispositivo en nFactor como componente EPA.

Verificación del certificado de dispositivo en un equipo Windows

1. Abra un explorador y acceda al FQDN de NetScaler Gateway.
2. Permita que se ejecute el cliente de Citrix End Point Analysis (EPA). Si aún no está instalado, instale la EPA.

   Citrix EPA ejecuta y valida el certificado de dispositivo y lo redirige a la página de autenticación si se aprueba la comprobación de EPA del certificado de dispositivo; de lo contrario, lo redirige a la página de error de la EPA. En caso de que tenga otras comprobaciones de la EPA, los resultados del análisis de la EPA dependen de las comprobaciones de la EPA configuradas.

Para realizar más depuraciones en el cliente, examine los siguientes registros de EPA en el cliente: C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

Nota:

> No se admite la verificación de certificados de dispositivo con CRL.

Importación e instalación de un certificado existente

March 27, 2024

Puede importar un certificado existente desde un equipo basado en Windows que ejecuta Internet Information Services (IIS) o desde un equipo que ejecuta Secure Gateway.

Al exportar el certificado, asegúrese de exportar también la clave privada. En ocasiones, no puede exportar la clave privada, lo que significa que no puede instalar el certificado en NetScaler Gateway. Si esto ocurre, utilice la solicitud de firma de certificado (CSR) para crear un certificado. Para obtener más información, consulte Creación de una solicitud de firma de certificado.

Al exportar un certificado y una clave privada de Windows, el equipo crea un archivo de intercambio de información personal (.pfx). Este archivo se instala en NetScaler Gateway como certificado PKCS #12.

Si va a reemplazar Secure Gateway por NetScaler Gateway, puede exportar el certificado y la clave privada desde Secure Gateway. Si realiza una migración local de Secure Gateway a NetScaler Gateway, el nombre de dominio completo (FQDN) de la aplicación y del dispositivo deben ser los mismos. Al exportar el certificado desde Secure Gateway, retira inmediatamente Secure Gateway, instala el certificado en NetScaler Gateway y, a continuación, prueba la configuración. Secure Gateway y NetScaler Gateway no pueden ejecutarse en la red al mismo tiempo si tienen el mismo FQDN.

Si utiliza Windows Server 2003 o Windows Server 2008, puede utilizar Microsoft Management Console para exportar el certificado. Para obtener más información, consulte la Ayuda en línea de Windows.

Deje los valores predeterminados para todas las demás opciones, defina una contraseña y guarde el archivo.pfx en el equipo. Cuando se exporta el certificado, lo instala en NetScaler Gateway.

Para instalar el certificado y la clave privada en NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en el **asistente de NetScaler Gateway** .
3. Haga clic en **Siguiente**, seleccione un servidor virtual existente y, a continuación, haga clic en **Siguiente**.
4. En **Opciones de certificado**, seleccione **Instalar un archivo PKCS#12 (.pfx)**.
5. En **Nombre de archivo PKCS #12**, haga clic en **Examinar**, vaya a el certificado y, a continuación, haga clic en **Seleccionar**.
6. En ((Contraseña)), escriba la contraseña de la clave privada.

   Esta es la contraseña que utilizó al convertir el certificado al formato PEM.
7. Haga clic en **Siguiente** para finalizar el asistente de NetScaler Gateway sin cambiar ninguna otra configuración.

Cuando el certificado está instalado en NetScaler Gateway, el certificado aparece en la utilidad de configuración del nodo **SSL\ > Certificados**.

Para crear una clave privada

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, haga clic en **SSL**.
2. En el panel de detalles, en **Claves SSL**, haga clic en **Crear clave RSA**.
3. En Nombre de**archivo clave**, escriba el nombre de la clave privada o haga clic en Examinar para ir a un archivo existente.
4. En**Tamaño de clave (bits)**, escriba el tamaño de la clave privada.
5. En**Valor de exponente público**, seleccione F4 o 3.

   El valor del exponente público de la clave RSA. Forma parte del algoritmo de cifrado y es necesario para crear la clave RSA. Los valores son F4 (Hex: 0x10001) o 3 (Hex: 0x3). El valor predeterminado es F4.
6. En**Formato clave**, seleccione PEM o DER. Citrix recomienda el formato PEM para el certificado.
7. En el **algoritmo de codificación PEM**, seleccione DES o DES3.
8. En**Frase de contraseña PEM** y **Verificar frase de contraseña**, escriba la contraseña, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

   Nota: Para asignar una frase de contraseña, el formato de clave debe ser PEM y debe seleccionar el algoritmo de codificación.

Para crear una clave privada de DSA en la utilidad de configuración, haga clic en**Crear clave DSA** y siga los pasos realizados para crear la clave privada RSA.

Listas de revocación de certificados

March 27, 2024

De vez en cuando, las entidades de certificación (CA) emiten listas de revocación de certificados (CRL). Las CRL contienen información sobre certificados en los que ya no se puede confiar. Por ejemplo, supongamos que Ann deja XYZ Corporation. La empresa puede colocar el certificado de Ann en una CRL para evitar que firme mensajes con esa clave.

Del mismo modo, puede revocar un certificado si una clave privada está en peligro o si ese certificado ha caducado y se está usando una nueva. Antes de confiar en una clave pública, asegúrese de que el certificado no aparezca en una CRL.

NetScaler Gateway admite los dos tipos de CRL siguientes:

- CRL que enumeran los certificados que se han revocado o que ya no son válidos
- Protocolo de estado de certificados en línea (OSCP), protocolo de Internet utilizado para obtener el estado de revocación de los certificados X.509

Para agregar una CRL:

Antes de configurar la CRL en el dispositivo NetScaler Gateway, asegúrese de que el archivo CRL se almacena localmente en el dispositivo. En el caso de una configuración de alta disponibilidad, el archivo CRL debe estar presente en ambos dispositivos NetScaler Gateway y la ruta de acceso del directorio al archivo debe ser la misma en ambos dispositivos.

Si necesita actualizar la CRL, puede utilizar los siguientes parámetros:

- Nombre de CRL: nombre de la CRL que se agrega en NetScaler. Máximo 31 caracteres.
- Archivo CRL: nombre del archivo CRL que se agrega en NetScaler. NetScaler busca el archivo CRL en el directorio /var/netscaler/ssl de forma predeterminada. Máximo 63 caracteres.
- URL: 127 caracteres como máximo
- DN base: 127 caracteres como máximo
- Enlazar DN: 127 caracteres como máximo
- Contraseña: 31 caracteres como máximo
- Días: máximo 31

1. En la utilidad de configuración, en la ficha Configuración, expanda SSL y, a continuación, haga clic en CRL.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Agregar CRL, especifique los valores de lo siguiente:
    - Nombre de CRL
    - Archivo CRL
    - Formato (opcional)
    - Certificado CA (opcional)
4. Haga clic en **Create** y, luego, en **Close**. En el panel de detalles de CRL, seleccione la CRL que ha configurado y compruebe que la configuración que aparece en la parte inferior de la pantalla es correcta.

Para configurar la actualización automática de CRL mediante LDAP o HTTP en la GUI:

Una entidad emisora de certificados genera y publica una CRL periódicamente o, a veces, inmediatamente después de revocar un certificado concreto. Citrix recomienda actualizar periódicamente las CRL del dispositivo NetScaler Gateway para protegerse de los clientes que intentan conectarse con certificados que no son válidos.

El dispositivo NetScaler Gateway puede actualizar CRL desde una ubicación web o un directorio LDAP. Cuando especifique parámetros de actualización y una ubicación web o un servidor LDAP, la CRL no tiene que estar presente en la unidad de disco duro local en el momento de ejecutar el comando. La primera actualización almacena una copia en la unidad de disco duro local, en la ruta especificada por el parámetro Archivo CRL. La ruta predeterminada para almacenar la CRL es /var/netscaler/ssl.

Parámetros de actualización de CRL

- **Nombre de CRL**

  Nombre de la CRL que se está actualizando en NetScaler Gateway.

- **Habilitar actualización automática de CRL**

  Habilite o inhabilite la actualización automática de CRL.

- **Certificado CA**

  Certificado de la entidad emisora de certificados que ha emitido la CRL. Este certificado de CA debe estar instalado en el dispositivo. El NetScaler solo puede actualizar CRL desde CA cuyos certificados están instalados en él.

- **Método**

  Protocolo para obtener la actualización de CRL de un servidor web (HTTP) o de un servidor LDAP. Valores posibles: HTTP, LDAP. Valor predeterminado: HTTP.

- **Ámbito**

  Extensión de la operación de búsqueda en el servidor LDAP. Si el ámbito especificado es Base, la búsqueda se encuentra al mismo nivel que el DN base. Si el ámbito especificado es Uno, la búsqueda se extiende a un nivel por debajo del DN base.

- **IP de servidor**

  Dirección IP del servidor LDAP del que se recupera la CRL. Seleccione IPv6 para utilizar una dirección IP IPv6.

- **Puerto**

  Número de puerto en el que se comunica el servidor LDAP o HTTP.

- **URL**

  Dirección URL de la ubicación web de la que se recupera la CRL.

- **DN base**

  DN base utilizado por el servidor LDAP para buscar el atributo CRL.
  Nota: Citrix recomienda utilizar el atributo DN base en lugar del nombre del emisor del certifi-

cado de CA para buscar la CRL en el servidor LDAP. Es posible que el campo Nombre del emisor no coincida exactamente con el DN de la estructura de directorios LDAP.

- **Vincular DN**

  El atributo bind DN se utiliza para acceder al objeto CRL del repositorio LDAP. Los atributos DN de enlace son las credenciales de administrador del servidor LDAP. Configure este parámetro para restringir el acceso no autorizado a los servidores LDAP.

- **Contraseña**

  Contraseña de administrador utilizada para acceder al objeto CRL del repositorio LDAP. Se requiere contraseña si el acceso al repositorio LDAP está restringido, es decir, no se permite el acceso anónimo.

- **Intervalo**

  Intervalo en el que se debe llevar a cabo la actualización de CRL. Para una actualización instantánea de CRL, especifique el intervalo como AHORA. Valores posibles: MENSUAL, DIARIO, SEMANAL, AHORA, NINGUNO.

- **Días**

  El día en que se debe realizar la actualización de la CRL. La opción no está disponible si el intervalo se establece en DIARIO.

- **Hora**

  Hora exacta en formato de 24 horas en la que se debe realizar la actualización de CRL.

- **Binario**

  Establezca el modo de recuperación de CRL basado en LDAP en binario. Valores posibles: SÍ, NO. Predeterminado: NO.

1. En el panel de navegación, expanda SSL y, a continuación, haga clic en CRL.
2. Seleccione la CRL configurada para la que quiere actualizar los parámetros de actualización y, a continuación, haga clic en Abrir.
3. Seleccione la opción Habilitar actualización automática de CRL.
4. En el grupo Parámetros de actualización automática de CRL, especifique valores para los siguientes parámetros:
   Nota: Un asterisco (*) indica un parámetro obligatorio.

   - Método
   - Binario
   - Ámbito
   - IP de servidor
   - Puerto*

- URL
- DNS base*
- Vincular DN
- Contraseña
- Intervalo
- Días
- Hora

5. Haga clic en Crear. En el panel CRL, seleccione la CRL que ha configurado y compruebe que la configuración que aparece en la parte inferior de la pantalla es correcta.

Supervisar el estado del certificado con OCSP

El Protocolo de estado de certificados en línea (OCSP) es un protocolo de Internet que se utiliza para determinar el estado de un certificado SSL de cliente. NetScaler Gateway admite OCSP según se define en RFC 2560. OCSP ofrece ventajas significativas sobre las listas de revocación de certificados (CRL) en términos de información oportuna. El estado de revocación actualizado de un certificado de cliente es especialmente útil en transacciones que implican grandes sumas de dinero y operaciones bursátiles de alto valor. También utiliza menos recursos del sistema y de la red. La implementación de OCSP en NetScaler Gateway incluye el procesamiento por lotes de solicitudes y el almacenamiento en caché de respuestas

Implementación de OCSP en NetScaler Gateway

La validación de OCSP en un dispositivo NetScaler Gateway comienza cuando NetScaler Gateway recibe un certificado de cliente durante un enlace SSL. Para validar el certificado, NetScaler Gateway crea una solicitud OCSP y la reenvía al respondedor OCSP. Para ello, NetScaler Gateway extrae la dirección URL del respondedor OCSP del certificado de cliente o utiliza una URL configurada localmente. La transacción está suspendida hasta que NetScaler Gateway evalúa la respuesta del servidor y determina si se permite o se rechaza la transacción. Si la respuesta del servidor se retrasa más allá del tiempo configurado y no hay ningún otro respondedor configurado, NetScaler Gateway permite la transacción o muestra un error, en función de si establece la comprobación de OCSP como opcional u obligatoria. NetScaler Gateway admite el procesamiento por lotes de solicitudes OCSP y el almacenamiento en caché de respuestas OCSP para reducir la carga del respondedor OCSP y proporcionar respuestas más rápidas.

procesamiento por lotes de solicitudes de OCSP

Cada vez que NetScaler Gateway recibe un certificado de cliente, envía una solicitud al respondedor OCSP. Para evitar sobrecargar el respondedor OCSP, NetScaler Gateway puede consultar el estado

de más de un certificado de cliente en la misma solicitud. Para que el procesamiento por lotes de solicitudes funcione de forma eficiente, es necesario definir un tiempo de espera para que el procesamiento de un único certificado no se retrase mientras se espera formar un lote.

Almacenamiento en caché de respuestas OCSP

El almacenamiento en caché de las respuestas recibidas del respondedor OCSP permite respuestas más rápidas para el usuario y reduce la carga del respondedor OCSP. Al recibir el estado de revocación de un certificado de cliente del respondedor OCSP, NetScaler Gateway almacena en caché la respuesta localmente durante un período de tiempo predefinido. Cuando se recibe un certificado de cliente durante un protocolo de enlace SSL, NetScaler Gateway comprueba primero su caché local en busca de una entrada para este certificado. Si se encuentra una entrada que sigue siendo válida (dentro del límite de tiempo de espera de la caché), se evalúa la entrada y se acepta o rechaza el certificado de cliente. Si no se encuentra un certificado, NetScaler Gateway envía una solicitud al respondedor OCSP y almacena la respuesta en su caché local durante un período de tiempo configurado.

Configurar el estado del certificado OCSP

La configuración de un Protocolo de estado de certificados en línea (OCSP) implica agregar un respondedor OCSP, vincular el respondedor OCSP a un certificado firmado de una entidad de certificación (CA) y vincular el certificado y la clave privada a un servidor virtual de Secure Sockets Layer (SSL). Si necesita vincular un certificado y una clave privada diferentes a un respondedor OCSP que ya ha configurado, primero debe desvincular el respondedor y, a continuación, enlazar el respondedor a un certificado diferente.

Para configurar OCSP

1. En la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Respondedor OCSP.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre , escriba un nombre para el perfil.
4. En URL, escriba la dirección web del respondedor OCSP.

   Este campo es obligatorio. La dirección web no puede superar los 32 caracteres.
5. Para almacenar en caché las respuestas de OCSP, haga clic en Caché y, en Tiempo de espera, escriba el número de minutos que NetScaler Gateway tiene la respuesta.
6. En Solicitar lote, haga clic en Habilitar.

7. En Retraso de procesamiento por lotes, especifique el tiempo, en milisegundos, permitido para agrupar por lotes un grupo de solicitudes OCSP.

   Los valores pueden ser de 0 a 10000. El valor predeterminado es 1.

8. En Sesgo producido en el momento, escriba la cantidad de tiempo que NetScaler Gateway puede utilizar cuando el dispositivo debe comprobar o aceptar la respuesta.

9. En Verificación de respuesta, seleccione Confiar en respuestas si quiere inhabilitar las comprobaciones de firma del respondedor de OCSP.

   Si habilita Respuestas de confianza, omita los pasos 8 y 9.

10. En Certificado, seleccione el certificado que se utiliza para firmar las respuestas de OCSP.

    Si no se selecciona un certificado, la CA a la que está vinculado el respondedor OCSP se utiliza para verificar las respuestas.

11. En Tiempo de espera de solicitud, escriba el número de milisegundos que debe esperar una respuesta de OCSP.

    Este tiempo incluye el tiempo de demora de procesamiento por lotes. Los valores pueden estar comprendidos entre 0 y 120000. El valor por defecto es 2000.

12. En Certificado de firma, seleccione el certificado y la clave privada utilizados para firmar las solicitudes de OCSP. Si no especifica un certificado ni una clave privada, las solicitudes no se firman.

13. Para habilitar el número usado una vez (`nonce`)`extension`, selecciona Nonce.

14. Para utilizar un certificado de cliente, haga clic en Inserción de certificados de cliente.

15. Haga clic en Create y, luego, en Close.

Administrar la configuración de NetScaler Gateway

January 26, 2024

Al realizar cambios de configuración en NetScaler Gateway, los cambios se guardan en archivos de registro. Puede ver varios tipos de ajustes de configuración:

- Configuración guardada. Puede ver la configuración que ha guardado en NetScaler Gateway.
- Configuración en ejecución. Puede ver la configuración activa, como un servidor virtual o una directiva de autenticación, que ha configurado pero que no ha guardado como configuración guardada en NetScaler Gateway.
- Configuración en ejecución versus configuración guardada. Puede comparar en paralelo la configuración en ejecución y guardada en NetScaler Gateway.

También puede borrar los valores de configuración de NetScaler Gateway.

Importante: Si decide borrar la configuración de NetScaler Gateway, se quitan los certificados, los servidores virtuales y las directivas. Citrix recomienda no borrar la configuración.

Guardar la configuración de NetScaler Gateway

Puede guardar la configuración actual de NetScaler Gateway en un equipo de la red, ver la configuración actual en ejecución y comparar las configuraciones guardadas y en ejecución.

Para guardar la configuración en NetScaler Gateway

1. En la utilidad de configuración, encima del panel de detalles, haga clic en el icono Guardar y, a continuación, haga clic en Sí.

Para ver y guardar el archivo de configuración en NetScaler Gateway

La configuración guardada es la configuración que se guarda en un archivo de registro de NetScaler Gateway, como la configuración de servidores virtuales, directivas, direcciones IP, usuarios, grupos y certificados.

Al configurar la configuración en NetScaler Gateway, puede guardarla en un archivo del equipo. Si necesita volver a instalar el software NetScaler Gateway o si elimina accidentalmente alguna configuración, puede utilizar este archivo para restaurar la configuración. Si necesita restaurar la configuración, puede copiar el archivo en NetScaler Gateway y reiniciar el dispositivo mediante la interfaz de línea de comandos o un programa, como WinSCP, para copiar el archivo en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Configuración guardada.
3. En el cuadro de diálogo Configuración guardada, haga clic en Guardar texto de salida en un archivo, asigne un nombre al archivo y, a continuación, haga clic en Guardar.
   Nota: Citrix recomienda guardar el archivo con el nombre de archivo ns.conf.

Para ver la configuración actual en ejecución

Cualquier cambio en NetScaler Gateway que se produzca sin esfuerzo por guardarlos se denomina configuración en ejecución. Esta configuración está activa en NetScaler Gateway, pero no se guarda en el dispositivo. Si ha configurado opciones adicionales, como una directiva, un servidor virtual, usuarios o grupos, puede ver esta configuración en la configuración en ejecución.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Configuración en ejecución.

Para comparar la configuración guardada y en ejecución

Puede ver qué configuración se guarda en el dispositivo y compararla con la configuración en ejecución. Puede elegir guardar la configuración en ejecución o realizar cambios en la configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Ver configuración, haga clic en Guardado v/s en ejecución.

Borrar la configuración de NetScaler Gateway

Puede borrar la configuración de NetScaler Gateway. Puede elegir entre los tres niveles de configuración siguientes para borrar:

Importante: Citrix recomienda guardar la configuración antes de borrar la configuración de NetScaler Gateway.

- Básico. Borra toda la configuración del dispositivo, excepto la dirección IP del sistema, la puerta de enlace predeterminada, las direcciones IP asignadas, las direcciones IP de subred, la configuración de DNS, la configuración de red, la configuración de alta disponibilidad, la contraseña administrativa y la configuración de funciones y modos.
- Extendida. Borra toda la configuración excepto la dirección IP del sistema, las direcciones IP asignadas, las direcciones IP de subred, la configuración DNS y las definiciones de alta disponibilidad.
- Completo. Restaura la configuración a la configuración original de fábrica, con exclusión de la dirección IP del sistema (NSIP) y la ruta predeterminada, necesarias para mantener la conectividad de red con el dispositivo.

Al borrar toda o parte de la configuración, la configuración de la función se establece en la configuración predeterminada de fábrica.

Al borrar la configuración, los archivos almacenados en NetScaler Gateway, como certificados y licencias, no se quitan. El archivo ns.conf no se modifica. Si quiere guardar la configuración antes de borrar la configuración, guarde la configuración en su equipo primero. Si guarda la configuración, puede restaurar el archivo ns.conf en NetScaler Gateway. Después de restaurar el archivo en el dispositivo y reiniciar NetScaler Gateway, se restaura cualquier configuración de ns.conf.

Las modificaciones de los archivos de configuración, como rc.conf, no se revierten.

Si tiene un par de alta disponibilidad, ambos dispositivos NetScaler Gateway se modifican de forma idéntica. Por ejemplo, si borra la configuración básica de un dispositivo, los cambios se propagan al segundo dispositivo.

Para borrar la configuración de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Diagnóstico.
2. En el panel de detalles, en Mantenimiento, haga clic en Borrar configuración.
3. En Nivel de configuración, seleccione el nivel que quiere borrar y, a continuación, haga clic en Ejecutar.

Administración de certificados en NetScaler Gateway

January 26, 2024

En NetScaler Gateway, utiliza certificados para crear conexiones seguras y autenticar usuarios.

Para establecer una conexión segura, se requiere un certificado de servidor en un extremo de la conexión. Se requiere un certificado raíz de la entidad emisora de certificados (CA) que emitió el certificado del servidor en el otro extremo de la conexión.

- Certificado de servidor. Un certificado de servidor certifica la identidad del servidor. NetScaler Gateway requiere este tipo de certificado digital.
- Certificado raíz. Un certificado raíz identifica a la CA que firmó el certificado de servidor. El certificado raíz pertenece a la entidad emisora de certificados. Un dispositivo de usuario requiere este tipo de certificado digital para verificar el certificado del servidor.

Al establecer una conexión segura con un explorador web en el dispositivo del usuario, el servidor envía su certificado al dispositivo.

Cuando el dispositivo de usuario recibe un certificado de servidor, el explorador web, como Internet Explorer, comprueba qué CA emitió el certificado y si el dispositivo del usuario confía en la entidad emisora de certificados. Si la entidad emisora de certificados no es de confianza o si se trata de un certificado de prueba, el explorador web solicita al usuario que acepte o rechace el certificado (aceptando o rechazando efectivamente la capacidad de acceder al sitio).

NetScaler Gateway admite los tres tipos de certificados siguientes:

- Certificado de prueba enlazado a un servidor virtual y que también se puede utilizar para conexiones a una comunidad de servidores. NetScaler Gateway incluye un certificado de prueba preinstalado.

- Certificado en formato PEM o DER firmado por una entidad emisora de certificados y emparejado con una clave privada.
- Certificado en formato PKCS #12 que se utiliza para almacenar o transportar el certificado y la clave privada. El certificado PKCS #12 se exporta normalmente de un certificado de Windows existente como archivo PFX y, a continuación, se instala en NetScaler Gateway.

Citrix recomienda utilizar un certificado firmado por una entidad emisora de certificados de confianza, como Thawte o Verisign.

Crear una solicitud de firma de certificado

March 27, 2024

Para proporcionar comunicaciones seguras mediante SSL o TLS, se requiere un certificado de servidor en NetScaler Gateway. Antes de cargar un certificado en NetScaler Gateway, debe generar una solicitud de firma de certificado (CSR) y una clave privada. Utilice la solicitud de creación de certificado incluida en el asistente de NetScaler Gateway o la utilidad de configuración para crear la CSR. La solicitud de creación de certificado crea un archivo.csr que se envía por correo electrónico a la entidad de certificación (CA) para que lo firme y una clave privada que permanece en el dispositivo. La CA firma el certificado y se lo devuelve a la dirección de correo electrónico que proporcionó. Cuando reciba el certificado firmado, podrá instalarlo en NetScaler Gateway. Cuando reciba el certificado de la entidad emisora de certificados, empareja el certificado con la clave privada.

Importante: Cuando utilice el asistente de NetScaler Gateway para crear la CSR, debe salir del asistente y esperar a que la CA le envíe el certificado firmado. Cuando reciba el certificado, puede volver a ejecutar el asistente de NetScaler Gateway para crear la configuración e instalar el certificado. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

Crear una CSR mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en el asistente de **NetScaler Gateway** .
3. Siga las instrucciones del asistente hasta llegar a la página Especificar un certificado de servidor.
4. Haga clic en **Crear una solicitud de firma de certificado** y complete los campos.
   Nota: El nombre de dominio completo (FQDN) no tiene por qué ser el mismo que el nombre de host de NetScaler Gateway. El FQDN se utiliza para el inicio de sesión del usuario.
5. Haga clic en **Crear** para guardar el certificado en el equipo y, a continuación, haga clic en **Cerrar**.

6. Salga del asistente de NetScaler Gateway sin guardar la configuración.

Crear una CSR mediante la GUI de NetScaler

También puede utilizar la GUI de NetScaler para crear una CSR sin ejecutar el asistente de NetScaler Gateway.

1. Vaya a **Administración de tráfico** > **SSL > Archivos SSL** y seleccione **Crear solicitud de firma de certificado (CSR)**.
2. Complete la configuración del certificado y, a continuación, haga clic en **Crear**.

Después de crear el certificado y la clave privada, envíe el certificado por correo electrónico a la CA, como Thawte o Verisign.

Para obtener información detallada sobre el procedimiento, consulte Crear una solicitud de firma de certificado.

Instalar el certificado firmado en NetScaler Gateway

Cuando reciba el certificado firmado de la entidad emisora de certificados (CA), emparéjelo con la clave privada del dispositivo y, a continuación, instale el certificado en NetScaler Gateway.

Empareja el certificado firmado con una clave privada mediante la interfaz gráfica de usuario

1. Copie el certificado en NetScaler Gateway en la carpeta nsconfig/ssl mediante un programa Secure Shell (SSH) como WinSCP.
2. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **SSL > Certificados**.
3. En la página **Certificado SSL**, haga clic en **Comenzar**.
4. En el panel de detalles, haga clic en **Instalar**.
5. En **Nombre del par de claves de certificado**, escriba el nombre del certificado.
6. En **Nombre de archivo de certificado**, haga clic **en Equipo**.
7. Vaya al certificado, haga clic en **Seleccionar** y, a continuación, en **Abrir**.
8. En **Nombre de archivo clave**, haga clic en **Equipo**. El nombre de la clave privada es el mismo que el de la solicitud de firma de certificado (CSR). La clave privada se encuentra en NetScaler Gateway en el directorio\ nsconfig\ ssl.
9. Elija la clave privada y, a continuación, haga clic en **Abrir**.
10. Si el certificado tiene formato PEM, en **Contraseña**, escriba la contraseña de la clave privada.
11. Si quiere configurar la notificación para cuándo caduca el certificado, seleccione **Notificar cuando caduque**.

12. En **Período de notificación**, escriba el número de días, haga clic en **Crear** y, a continuación, en **Cerrar**.

Enlazar el certificado y la clave privada a un servidor virtual mediante la interfaz gráfica de usuario

Después de crear y vincular un par de certificados y claves privadas, enlaza a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Certificados, en **Disponible**, seleccione un certificado, haga clic en **Agregar** y, a continuación, en **Aceptar**.

Enlazar el certificado y la clave privada a un servidor virtual mediante la CLI

En la línea de comandos, escriba;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
   Mandatory | Optional )
<!--NeedCopy-->
```

Ejemplo:

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
   ocspCheck Mandatory
<!--NeedCopy-->
```

Nota: OscpCheck es opcional si la comprobación OCSP no es necesaria para el certificado del dispositivo.

Desvincular certificados de prueba del servidor virtual mediante la interfaz gráfica de usuario

Después de instalar el certificado firmado, desvincule todos los certificados de prueba vinculados al servidor virtual. Puede desvincular certificados de prueba mediante la utilidad de configuración.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Certificados, en **Configurado**, seleccione el certificado de prueba y, a continuación, haga clic en **Quitar**.

Configurar certificados intermedios

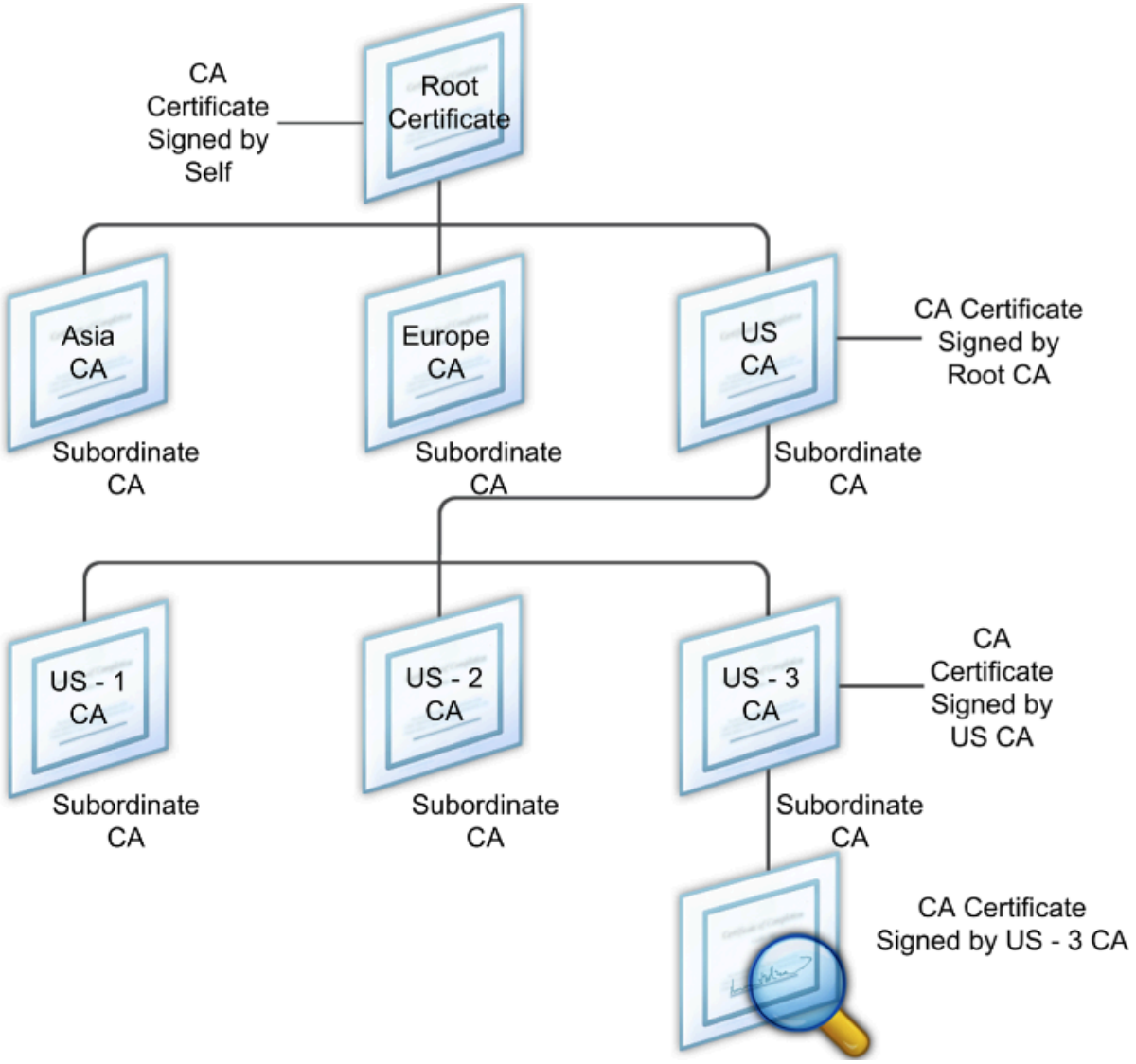
January 26, 2024

Un certificado intermedio es un certificado que va entre NetScaler Gateway (el certificado del servidor) y un certificado raíz (instalado en el dispositivo del usuario). Un certificado intermedio forma parte de una cadena.

Algunas organizaciones delegan la responsabilidad de emitir certificados para resolver el problema de la separación geográfica entre las unidades organizativas o para aplicar directivas de emisión diferentes a distintas secciones de la organización.

La responsabilidad de la emisión de certificados se puede delegar mediante la configuración de entidades de certificación (CA) subordinadas. Las entidades emisoras de certificados pueden firmar sus propios certificados (es decir, están autofirmados) o pueden firmarlos otra entidad emisora de certificados. El estándar X.509 incluye un modelo para configurar una jerarquía de CA. En este modelo, como se muestra en la siguiente ilustración, la CA raíz se encuentra en la parte superior de la jerarquía y es un certificado autofirmado por la entidad emisora de certificados. Las entidades emisoras de certificados que están directamente subordinadas a la entidad emisora de certificados raíz tienen certificados de CA firmados por la entidad emisora de certificados raíz. Las entidades emisoras de certificados subordinadas de la jerarquía tienen sus certificados de CA firmados por las entidades emisoras de certificados subordinadas.

Figura 1. El modelo X.509 muestra la estructura jerárquica de una cadena de certificados digitales típica



Si un certificado de servidor está firmado por una CA con un certificado autofirmado, la cadena de certificados se compone exactamente de dos certificados: el certificado de entidad final y la entidad emisora de certificados raíz. Si un certificado de usuario o servidor está firmado por una entidad emisora de certificados intermedia, la cadena de certificados es más larga.

En la siguiente ilustración se muestra que los dos primeros elementos son el certificado de entidad final (en este caso, gwy01.company.com) y el certificado de la entidad emisora de certificados intermedia, en ese orden. El certificado de la entidad emisora de certificados intermedia va seguido del certificado de su entidad emisora de certificados. Esta lista continúa hasta que el último certificado de la lista corresponde a una entidad emisora de certificados raíz. Cada certificado de la cadena da fe de la identidad del certificado anterior.

Figura 2. Una cadena de certificados digitales típica

Instalar un certificado intermedio

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, haga clic en Instalar.
3. En Nombre del par de claves de certificado, escriba el nombre del certificado.
4. En Detalles, en Nombre de archivo de certificado, haga clic en Examinar (dispositivo) y, en la lista, seleccione Local o Equipo.
5. Vaya a el certificado en su equipo (local) o en NetScaler Gateway (dispositivo).
6. En Formato de certificado, seleccione PEM.
7. Haga clic en Instalar y, a continuación, en Cerrar.

Al instalar un certificado intermedio en NetScaler Gateway, no es necesario especificar la clave privada ni la contraseña.

Una vez instalado el certificado en el dispositivo, el certificado debe vincularse al certificado del servidor.

Vincular un certificado intermedio a un certificado de servidor

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, seleccione el certificado de servidor y, a continuación, en Acción, haga clic en Vincular.
3. Junto a Nombre del certificado de CA, seleccione el certificado intermedio de la lista y, a continuación, haga clic en Aceptar.

Usar certificados de dispositivo para la autenticación

January 26, 2024

NetScaler Gateway admite la comprobación de certificados de dispositivo que permite vincular la identidad del dispositivo a la clave privada de un certificado. La comprobación del certificado del dispositivo se puede configurar como parte de las directivas clásicas o avanzadas de Endpoint Analysis (EPA). En las directivas clásicas de EPA, el certificado de dispositivo solo se puede configurar para la EPA de autenticación previa.

NetScaler Gateway verifica el certificado del dispositivo antes de que se ejecute el análisis de endpoint o antes de que aparezca la página de inicio de sesión. Si configura el análisis de endpoints, el análisis de endpoints se ejecuta para verificar el dispositivo del usuario. Cuando el dispositivo pasa el análisis y después de que NetScaler Gateway verifica el certificado del dispositivo, los usuarios pueden iniciar sesión en NetScaler Gateway.

> **Importante:**
>
> - De forma predeterminada, Windows exige privilegios de administrador para acceder a los certificados de dispositivo.
> - Para agregar una comprobación de certificado de dispositivo para usuarios que no son administradores, debe instalar el complemento VPN. La versión del plug-in VPN debe ser la misma que el plug-in de la EPA del dispositivo.
> - Puede agregar varios certificados de CA a la puerta de enlace y validar el certificado de dispositivo.
> - Si instala dos o más certificados de dispositivo en NetScaler Gateway, los usuarios deben seleccionar el certificado correcto cuando empiecen a iniciar sesión en NetScaler Gateway o antes de que se ejecute el análisis de endpoint.
> - Al crear el certificado de dispositivo, debe ser un certificado X.509.
> - Si tiene un certificado de dispositivo emitido por una CA intermedia, los certificados de CA intermedia y raíz deben estar vinculados.
> - El cliente EPA necesita que el usuario tenga derechos de administrador local para poder acceder al almacén de certificados de la máquina. Esto rara vez ocurre, por lo que una solución alternativa es instalar el complemento completo de NetScaler Gateway que puede acceder al almacén local.

Para obtener más información sobre cómo crear certificados de dispositivo, consulte lo siguiente:

- Servicio de inscripción de dispositivos de red (NDES) en los Servicios de certificados de Active Directory (AD CS) en el sitio web de Microsoft.
- Cómo solicitar un certificado a una entidad emisora de certificados de Microsoft mediante DCE/RPC y la carga útil del perfil de certificados de Active Directory en el sitio web de soporte técnico de Apple.
- Emisión de certificados iPad o iPhone en el blog de soporte técnico de Microsoft Pregunte al equipo de servicios de directorio.
- Configuración del servicio de inscripción de dispositivos de red en el sitio web de TI Pro de

Windows.

- Ejemplo paso a paso de implementación de certificados PKI para Configuration Manager: ¿Entidad de certificación de Windows Server 2008? RedirectedFrom=MSDN) en el sitio web de Microsoft System Center.

Pasos para configurar certificados de dispositivo

Para configurar un certificado de dispositivo, debe completar los pasos siguientes:

- Instale el certificado de entidad emisora de certificados del dispositivo en NetScaler Gateway. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Enlace el certificado de entidad emisora de certificados del dispositivo al servidor virtual de NetScaler Gateway y habilite la comprobación de OCSP. Para obtener más información, consulte Instalación del certificado firmado en NetScaler Gateway.
- Cree y vincule OCSP (respondedor) en el certificado de entidad emisora de certificados del dispositivo. Para obtener más información, consulte Supervisar el estado de los certificados con OCSP.

Habilite la comprobación de certificados de dispositivo en el servidor virtual y agregue el certificado de entidad emisora de certificados de dispositivo a la lista de comprobación de certificados de dispositivo. Para obtener más información, consulte Habilitar la comprobación de certificados de dispositivo en un servidor virtual para la directiva clásica de EPA.

Complete la configuración del cliente y la verificación del certificado de dispositivo en la máquina Windows. Para obtener más información, consulte Verificación del certificado de dispositivo en un equipo Windows.

> **Nota:**
>
> Todos los clientes destinados a aprovechar la comprobación EPA del certificado de dispositivo deben tener el certificado de dispositivo instalado en el almacén de certificados del sistema de la máquina.

Habilitar la comprobación de certificados de dispositivo en un servidor virtual para la directiva clásica de EPA

Después de crear el certificado de dispositivo, instale el certificado en NetScaler Gateway mediante el procedimiento de importación e instalación de un certificado existente en NetScaler Gateway.

1. En la pestaña Configuración, vaya a **NetScaler Gateway > Servidores virtuales**.

2. En la página **Servidores virtuales de NetScaler Gateway**, seleccione un servidor virtual existente y haga clic en **Editar**.
3. En la página **Servidores virtuales VPN** , en la sección **Configuración básica** , haga clic en **Editar** .
4. Desactive la casilla **Habilitar autenticación** para inhabilitar la autenticación.
5. Seleccione la casilla **Habilitar certificado de dispositivo** para habilitar el certificado de dispositivo
6. Haga clic en **Agregar** para agregar a la lista el nombre del certificado de entidad emisora de certificados de dispositivo disponible.
7. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **CA para certificado de dispositivo**, haga clic en **Agregar**, seleccione el certificado y, a continuación, haga clic en **+**.

> **Nota:**
>
> Para obtener información sobre cómo habilitar y vincular certificados de dispositivo en un servidor virtual para directivas EPA avanzadas, consulte Certificado de dispositivo en nFactor como componente EPA.

Verificación del certificado de dispositivo en un equipo Windows

1. Abra un explorador y acceda al FQDN de NetScaler Gateway.
2. Permita que se ejecute el cliente de Citrix End Point Analysis (EPA). Si aún no está instalado, instale la EPA.

   Citrix EPA ejecuta y valida el certificado de dispositivo y lo redirige a la página de autenticación si se aprueba la comprobación de EPA del certificado de dispositivo; de lo contrario, lo redirige a la página de error de la EPA. En caso de que tenga otras comprobaciones de la EPA, los resultados del análisis de la EPA dependen de las comprobaciones de la EPA configuradas.

Para realizar más depuraciones en el cliente, examine los siguientes registros de EPA en el cliente: C:\Users<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

Nota:

> No se admite la verificación de certificados de dispositivo con CRL.

Importación e instalación de un certificado existente

March 27, 2024

Puede importar un certificado existente desde un equipo basado en Windows que ejecuta Internet Information Services (IIS) o desde un equipo que ejecuta Secure Gateway.

Al exportar el certificado, asegúrese de exportar también la clave privada. En ocasiones, no puede exportar la clave privada, lo que significa que no puede instalar el certificado en NetScaler Gateway. Si esto ocurre, utilice la solicitud de firma de certificado (CSR) para crear un certificado. Para obtener más información, consulte Creación de una solicitud de firma de certificado.

Al exportar un certificado y una clave privada de Windows, el equipo crea un archivo de intercambio de información personal (.pfx). Este archivo se instala en NetScaler Gateway como certificado PKCS #12.

Si va a reemplazar Secure Gateway por NetScaler Gateway, puede exportar el certificado y la clave privada desde Secure Gateway. Si realiza una migración local de Secure Gateway a NetScaler Gateway, el nombre de dominio completo (FQDN) de la aplicación y del dispositivo deben ser los mismos. Al exportar el certificado desde Secure Gateway, retira inmediatamente Secure Gateway, instala el certificado en NetScaler Gateway y, a continuación, prueba la configuración. Secure Gateway y NetScaler Gateway no pueden ejecutarse en la red al mismo tiempo si tienen el mismo FQDN.

Si utiliza Windows Server 2003 o Windows Server 2008, puede utilizar Microsoft Management Console para exportar el certificado. Para obtener más información, consulte la Ayuda en línea de Windows.

Deje los valores predeterminados para todas las demás opciones, defina una contraseña y guarde el archivo.pfx en el equipo. Cuando se exporta el certificado, lo instala en NetScaler Gateway.

Para instalar el certificado y la clave privada en NetScaler Gateway

1. En la utilidad de configuración, haga clic en la ficha Configuración y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Introducción, haga clic en el **asistente de NetScaler Gateway** .
3. Haga clic en **Siguiente**, seleccione un servidor virtual existente y, a continuación, haga clic en **Siguiente**.
4. En **Opciones de certificado**, seleccione **Instalar un archivo PKCS#12 (.pfx)**.
5. En **Nombre de archivo PKCS #12**, haga clic en **Examinar**, vaya a el certificado y, a continuación, haga clic en **Seleccionar**.
6. En ((Contraseña)), escriba la contraseña de la clave privada.

   Esta es la contraseña que utilizó al convertir el certificado al formato PEM.
7. Haga clic en **Siguiente** para finalizar el asistente de NetScaler Gateway sin cambiar ninguna otra configuración.

Cuando el certificado está instalado en NetScaler Gateway, el certificado aparece en la utilidad de configuración del nodo **SSL\ > Certificados**.

Para crear una clave privada

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, haga clic en **SSL**.
2. En el panel de detalles, en **Claves SSL**, haga clic en **Crear clave RSA**.
3. En Nombre de**archivo clave**, escriba el nombre de la clave privada o haga clic en Examinar para ir a un archivo existente.
4. En**Tamaño de clave (bits)**, escriba el tamaño de la clave privada.
5. En**Valor de exponente público**, seleccione F4 o 3.

   El valor del exponente público de la clave RSA. Forma parte del algoritmo de cifrado y es necesario para crear la clave RSA. Los valores son F4 (Hex: 0x10001) o 3 (Hex: 0x3). El valor predeterminado es F4.
6. En**Formato clave**, seleccione PEM o DER. Citrix recomienda el formato PEM para el certificado.
7. En el **algoritmo de codificación PEM**, seleccione DES o DES3.
8. En**Frase de contraseña PEM** y **Verificar frase de contraseña**, escriba la contraseña, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

   Nota: Para asignar una frase de contraseña, el formato de clave debe ser PEM y debe seleccionar el algoritmo de codificación.

Para crear una clave privada de DSA en la utilidad de configuración, haga clic en**Crear clave DSA** y siga los pasos realizados para crear la clave privada RSA.

Listas de revocación de certificados

March 27, 2024

De vez en cuando, las entidades de certificación (CA) emiten listas de revocación de certificados (CRL). Las CRL contienen información sobre certificados en los que ya no se puede confiar. Por ejemplo, supongamos que Ann deja XYZ Corporation. La empresa puede colocar el certificado de Ann en una CRL para evitar que firme mensajes con esa clave.

Del mismo modo, puede revocar un certificado si una clave privada está en peligro o si ese certificado ha caducado y se está usando una nueva. Antes de confiar en una clave pública, asegúrese de que el certificado no aparezca en una CRL.

NetScaler Gateway admite los dos tipos de CRL siguientes:

- CRL que enumeran los certificados que se han revocado o que ya no son válidos
- Protocolo de estado de certificados en línea (OSCP), protocolo de Internet utilizado para obtener el estado de revocación de los certificados X.509

Para agregar una CRL:

Antes de configurar la CRL en el dispositivo NetScaler Gateway, asegúrese de que el archivo CRL se almacena localmente en el dispositivo. En el caso de una configuración de alta disponibilidad, el archivo CRL debe estar presente en ambos dispositivos NetScaler Gateway y la ruta de acceso del directorio al archivo debe ser la misma en ambos dispositivos.

Si necesita actualizar la CRL, puede utilizar los siguientes parámetros:

- Nombre de CRL: nombre de la CRL que se agrega en NetScaler. Máximo 31 caracteres.
- Archivo CRL: nombre del archivo CRL que se agrega en NetScaler. NetScaler busca el archivo CRL en el directorio /var/netscaler/ssl de forma predeterminada. Máximo 63 caracteres.
- URL: 127 caracteres como máximo
- DN base: 127 caracteres como máximo
- Enlazar DN: 127 caracteres como máximo
- Contraseña: 31 caracteres como máximo
- Días: máximo 31

1. En la utilidad de configuración, en la ficha Configuración, expanda SSL y, a continuación, haga clic en CRL.
2. En el panel de detalles, haga clic en Agregar.
3. En el cuadro de diálogo Agregar CRL, especifique los valores de lo siguiente:
    - Nombre de CRL
    - Archivo CRL
    - Formato (opcional)
    - Certificado CA (opcional)
4. Haga clic en **Create** y, luego, en **Close**. En el panel de detalles de CRL, seleccione la CRL que ha configurado y compruebe que la configuración que aparece en la parte inferior de la pantalla es correcta.

Para configurar la actualización automática de CRL mediante LDAP o HTTP en la GUI:

Una entidad emisora de certificados genera y publica una CRL periódicamente o, a veces, inmediatamente después de revocar un certificado concreto. Citrix recomienda actualizar periódicamente las CRL del dispositivo NetScaler Gateway para protegerse de los clientes que intentan conectarse con certificados que no son válidos.

El dispositivo NetScaler Gateway puede actualizar CRL desde una ubicación web o un directorio LDAP. Cuando especifique parámetros de actualización y una ubicación web o un servidor LDAP, la CRL no tiene que estar presente en la unidad de disco duro local en el momento de ejecutar el comando. La primera actualización almacena una copia en la unidad de disco duro local, en la ruta especificada por el parámetro Archivo CRL. La ruta predeterminada para almacenar la CRL es /var/netscaler/ssl.

Parámetros de actualización de CRL

- **Nombre de CRL**

  Nombre de la CRL que se está actualizando en NetScaler Gateway.

- **Habilitar actualización automática de CRL**

  Habilite o inhabilite la actualización automática de CRL.

- **Certificado CA**

  Certificado de la entidad emisora de certificados que ha emitido la CRL. Este certificado de CA debe estar instalado en el dispositivo. El NetScaler solo puede actualizar CRL desde CA cuyos certificados están instalados en él.

- **Método**

  Protocolo para obtener la actualización de CRL de un servidor web (HTTP) o de un servidor LDAP. Valores posibles: HTTP, LDAP. Valor predeterminado: HTTP.

- **Ámbito**

  Extensión de la operación de búsqueda en el servidor LDAP. Si el ámbito especificado es Base, la búsqueda se encuentra al mismo nivel que el DN base. Si el ámbito especificado es Uno, la búsqueda se extiende a un nivel por debajo del DN base.

- **IP de servidor**

  Dirección IP del servidor LDAP del que se recupera la CRL. Seleccione IPv6 para utilizar una dirección IP IPv6.

- **Puerto**

  Número de puerto en el que se comunica el servidor LDAP o HTTP.

- **URL**

  Dirección URL de la ubicación web de la que se recupera la CRL.

- **DN base**

  DN base utilizado por el servidor LDAP para buscar el atributo CRL.
  Nota: Citrix recomienda utilizar el atributo DN base en lugar del nombre del emisor del certifi-

cado de CA para buscar la CRL en el servidor LDAP. Es posible que el campo Nombre del emisor no coincida exactamente con el DN de la estructura de directorios LDAP.

- **Vincular DN**

  El atributo bind DN se utiliza para acceder al objeto CRL del repositorio LDAP. Los atributos DN de enlace son las credenciales de administrador del servidor LDAP. Configure este parámetro para restringir el acceso no autorizado a los servidores LDAP.

- **Contraseña**

  Contraseña de administrador utilizada para acceder al objeto CRL del repositorio LDAP. Se requiere contraseña si el acceso al repositorio LDAP está restringido, es decir, no se permite el acceso anónimo.

- **Intervalo**

  Intervalo en el que se debe llevar a cabo la actualización de CRL. Para una actualización instantánea de CRL, especifique el intervalo como AHORA. Valores posibles: MENSUAL, DIARIO, SEMANAL, AHORA, NINGUNO.

- **Días**

  El día en que se debe realizar la actualización de la CRL. La opción no está disponible si el intervalo se establece en DIARIO.

- **Hora**

  Hora exacta en formato de 24 horas en la que se debe realizar la actualización de CRL.

- **Binario**

  Establezca el modo de recuperación de CRL basado en LDAP en binario. Valores posibles: SÍ, NO. Predeterminado: NO.

1. En el panel de navegación, expanda SSL y, a continuación, haga clic en CRL.
2. Seleccione la CRL configurada para la que quiere actualizar los parámetros de actualización y, a continuación, haga clic en Abrir.
3. Seleccione la opción Habilitar actualización automática de CRL.
4. En el grupo Parámetros de actualización automática de CRL, especifique valores para los siguientes parámetros:
   Nota: Un asterisco (*) indica un parámetro obligatorio.

   - Método
   - Binario
   - Ámbito
   - IP de servidor
   - Puerto*

- URL
- DNS base*
- Vincular DN
- Contraseña
- Intervalo
- Días
- Hora

5. Haga clic en Crear. En el panel CRL, seleccione la CRL que ha configurado y compruebe que la configuración que aparece en la parte inferior de la pantalla es correcta.

Supervisar el estado del certificado con OCSP

El Protocolo de estado de certificados en línea (OCSP) es un protocolo de Internet que se utiliza para determinar el estado de un certificado SSL de cliente. NetScaler Gateway admite OCSP según se define en RFC 2560. OCSP ofrece ventajas significativas sobre las listas de revocación de certificados (CRL) en términos de información oportuna. El estado de revocación actualizado de un certificado de cliente es especialmente útil en transacciones que implican grandes sumas de dinero y operaciones bursátiles de alto valor. También utiliza menos recursos del sistema y de la red. La implementación de OCSP en NetScaler Gateway incluye el procesamiento por lotes de solicitudes y el almacenamiento en caché de respuestas

Implementación de OCSP en NetScaler Gateway

La validación de OCSP en un dispositivo NetScaler Gateway comienza cuando NetScaler Gateway recibe un certificado de cliente durante un enlace SSL. Para validar el certificado, NetScaler Gateway crea una solicitud OCSP y la reenvía al respondedor OCSP. Para ello, NetScaler Gateway extrae la dirección URL del respondedor OCSP del certificado de cliente o utiliza una URL configurada localmente. La transacción está suspendida hasta que NetScaler Gateway evalúa la respuesta del servidor y determina si se permite o se rechaza la transacción. Si la respuesta del servidor se retrasa más allá del tiempo configurado y no hay ningún otro respondedor configurado, NetScaler Gateway permite la transacción o muestra un error, en función de si establece la comprobación de OCSP como opcional u obligatoria. NetScaler Gateway admite el procesamiento por lotes de solicitudes OCSP y el almacenamiento en caché de respuestas OCSP para reducir la carga del respondedor OCSP y proporcionar respuestas más rápidas.

procesamiento por lotes de solicitudes de OCSP

Cada vez que NetScaler Gateway recibe un certificado de cliente, envía una solicitud al respondedor OCSP. Para evitar sobrecargar el respondedor OCSP, NetScaler Gateway puede consultar el estado

de más de un certificado de cliente en la misma solicitud. Para que el procesamiento por lotes de solicitudes funcione de forma eficiente, es necesario definir un tiempo de espera para que el procesamiento de un único certificado no se retrase mientras se espera formar un lote.

Almacenamiento en caché de respuestas OCSP

El almacenamiento en caché de las respuestas recibidas del respondedor OCSP permite respuestas más rápidas para el usuario y reduce la carga del respondedor OCSP. Al recibir el estado de revocación de un certificado de cliente del respondedor OCSP, NetScaler Gateway almacena en caché la respuesta localmente durante un período de tiempo predefinido. Cuando se recibe un certificado de cliente durante un protocolo de enlace SSL, NetScaler Gateway comprueba primero su caché local en busca de una entrada para este certificado. Si se encuentra una entrada que sigue siendo válida (dentro del límite de tiempo de espera de la caché), se evalúa la entrada y se acepta o rechaza el certificado de cliente. Si no se encuentra un certificado, NetScaler Gateway envía una solicitud al respondedor OCSP y almacena la respuesta en su caché local durante un período de tiempo configurado.

Configurar el estado del certificado OCSP

La configuración de un Protocolo de estado de certificados en línea (OCSP) implica agregar un respondedor OCSP, vincular el respondedor OCSP a un certificado firmado de una entidad de certificación (CA) y vincular el certificado y la clave privada a un servidor virtual de Secure Sockets Layer (SSL). Si necesita vincular un certificado y una clave privada diferentes a un respondedor OCSP que ya ha configurado, primero debe desvincular el respondedor y, a continuación, enlazar el respondedor a un certificado diferente.

Para configurar OCSP

1. En la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Respondedor OCSP.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre , escriba un nombre para el perfil.
4. En URL, escriba la dirección web del respondedor OCSP.

   Este campo es obligatorio. La dirección web no puede superar los 32 caracteres.
5. Para almacenar en caché las respuestas de OCSP, haga clic en Caché y, en Tiempo de espera, escriba el número de minutos que NetScaler Gateway tiene la respuesta.
6. En Solicitar lote, haga clic en Habilitar.

7. En Retraso de procesamiento por lotes, especifique el tiempo, en milisegundos, permitido para agrupar por lotes un grupo de solicitudes OCSP.

   Los valores pueden ser de 0 a 10000. El valor predeterminado es 1.

8. En Sesgo producido en el momento, escriba la cantidad de tiempo que NetScaler Gateway puede utilizar cuando el dispositivo debe comprobar o aceptar la respuesta.

9. En Verificación de respuesta, seleccione Confiar en respuestas si quiere inhabilitar las comprobaciones de firma del respondedor de OCSP.

   Si habilita Respuestas de confianza, omita los pasos 8 y 9.

10. En Certificado, seleccione el certificado que se utiliza para firmar las respuestas de OCSP.

    Si no se selecciona un certificado, la CA a la que está vinculado el respondedor OCSP se utiliza para verificar las respuestas.

11. En Tiempo de espera de solicitud, escriba el número de milisegundos que debe esperar una respuesta de OCSP.

    Este tiempo incluye el tiempo de demora de procesamiento por lotes. Los valores pueden estar comprendidos entre 0 y 120000. El valor por defecto es 2000.

12. En Certificado de firma, seleccione el certificado y la clave privada utilizados para firmar las solicitudes de OCSP. Si no especifica un certificado ni una clave privada, las solicitudes no se firman.

13. Para habilitar el número usado una vez (`nonce`)`extension`, selecciona Nonce.

14. Para utilizar un certificado de cliente, haga clic en Inserción de certificados de cliente.

15. Haga clic en Create y, luego, en Close.

Pruebe la configuración de NetScaler Gateway

March 27, 2024

Después de configurar la configuración inicial en NetScaler Gateway, puede probar la configuración conectándose al dispositivo.

Para probar la configuración de NetScaler Gateway, cree una cuenta de usuario local. A continuación, utilice la dirección IP del servidor virtual o el nombre de dominio completo (FQDN) del dispositivo, abra un explorador Web y escriba la dirección web. Por ejemplo, en la barra de direcciones, escriba`https://my.company.com` o`https://192.168.96.183`.

En la pantalla de inicio de sesión, introduzca el nombre de usuario y la contraseña de la cuenta de usuario que creó anteriormente. Tras iniciar sesión, se le solicitará que descargue e instale el cliente Citrix Secure Access.

Tras instalar el cliente Citrix Secure Access y conectarse correctamente con él, aparece la interfaz de acceso. La interfaz de acceso es la página principal predeterminada de NetScaler Gateway.

Crear una cuenta de usuario mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway\ > Administración de usuarios**y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, haga clic en Agregar.
3. En Nombre de usuario, escriba el nombre de usuario.
4. Si utiliza la autenticación local, desactive la casilla Autenticación externa. La autenticación de usuarios con tipos de autenticación externa, como LDAP o RADIUS, es la opción predeterminada. Si desactiva esta casilla de verificación, NetScaler Gateway autentica a los usuarios.
5. En Contraseña y Confirmar contraseña, escriba la contraseña del usuario, haga clic en Crear y, a continuación, en Cerrar .

Al agregar usuarios mediante la utilidad de configuración, puede enlazar las siguientes directivas al usuario:

- Autorización
- Tráfico, sesión y auditoría
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

Si tiene problemas para iniciar sesión con la cuenta de usuario de prueba, compruebe lo siguiente:

- Si recibe una advertencia de certificado, se instala un certificado de prueba o un certificado no válido en NetScaler Gateway. Si hay un certificado firmado por una entidad de certificación (CA) instalado en el dispositivo, asegúrese de que haya un certificado raíz correspondiente en el dispositivo del usuario.
- Si utilizó un certificado firmado por una entidad emisora de certificados, compruebe que ha generado el certificado de sitio correctamente mediante la solicitud de firma de certificado (CSR) firmada y que los datos de nombre distintivo (DN) introducidos en la CSR son correctos. El problema también puede ser que el nombre de host no coincida con la dirección IP que figura en el certificado firmado. Compruebe que el nombre común del certificado configurado corresponde a la información de dirección IP del servidor virtual configurado.

- Si no aparece la pantalla de inicio de sesión o si aparece algún otro mensaje de error, revise el proceso de configuración y confirme que ha realizado todos los pasos correctamente y que ha introducido todos los parámetros correctamente.

Actualización del software NetScaler Gateway

January 26, 2024

Puede actualizar el software que reside en NetScaler Gateway cuando haya nuevas versiones disponibles. Puede buscar actualizaciones en el sitio web de Citrix. Solo puede actualizar a una nueva versión si sus licencias de NetScaler Gateway están bajo el programa Subscription Advantage cuando se publique la actualización. Puede renovar Subscription Advantage en cualquier momento. Para obtener más información, consulte el sitio web de soporte de NetScaler.

La ruta de actualización y la información de productos compatibles también están disponibles en la Guía de actualización de Citrix.

Para obtener información sobre la última versión de mantenimiento de NetScaler Gateway, consulte Citrix Knowledge Center.

Buscar actualizaciones de software

1. Vaya al sitio Web de Citrix.
2. Haga clic en **My Account** e inicie sesión.
3. Haga clic en **Descargas**.
4. En Buscar descargas, seleccione **NetScaler Gateway**.
5. En **Seleccionar tipo de descarga**, seleccione **Software del producto** y, a continuación, haga clic en **Buscar**.
   También puede seleccionar **Virtual Appliances** para descargar NetScaler VPX. Cuando se selecciona esta opción, se recibe una lista de software para la máquina virtual para cada hipervisor.
6. En la página NetScaler Gateway, expanda **NetScaler Gateway o Access Gateway**.
7. Haga clic en la versión del software de dispositivo que quiere descargar.
8. En la página del software del dispositivo de la versión que quiere descargar, seleccione el dispositivo virtual y, a continuación, haga clic en **Descargar**.
9. Siga las instrucciones en pantalla para descargar el software.

Cuando se descarga el software en el equipo, puede utilizar el Asistente de actualización o el símbolo del sistema para instalar el software.

Actualizar NetScaler Gateway mediante el Asistente de actualización

1. En la utilidad de configuración, en la **ficha Configuración**, en el panel de navegación, haga clic en Sistema.
2. En el panel de detalles, haga clic en **Asistente de actualización**.
3. Haga clic en **Next** y siga las instrucciones del asistente.

Actualizar NetScaler Gateway mediante un símbolo del sistema

1. Para cargar el software en NetScaler Gateway, utilice un cliente FTP seguro, como WinSCP, para conectarse al dispositivo.
2. Copie el software del equipo en el`nsinstall` directorio /var/ del dispositivo.
3. Utilice un cliente de Secure Shell (SSH), como PuTTY, para abrir una conexión SSH con el dispositivo.
4. Inicie sesión en NetScaler Gateway.
5. En una línea de comandos, escriba: `shell`
6. Para cambiar al directorio `nsinstall`, en el símbolo del sistema, escriba: `cd /var/nsinstall`
7. Para ver el contenido del directorio, escriba: `ls`
8. Para descomprimir el software, escriba: tar —xvzf build_x_xx.tgz, donde build_x_xx.tgz es el nombre de la compilación a la que quiere actualizar.
9. Para iniciar la instalación, en el símbolo del sistema, escriba: `./installns`
10. Cuando finalice la instalación, reinicie NetScaler Gateway.

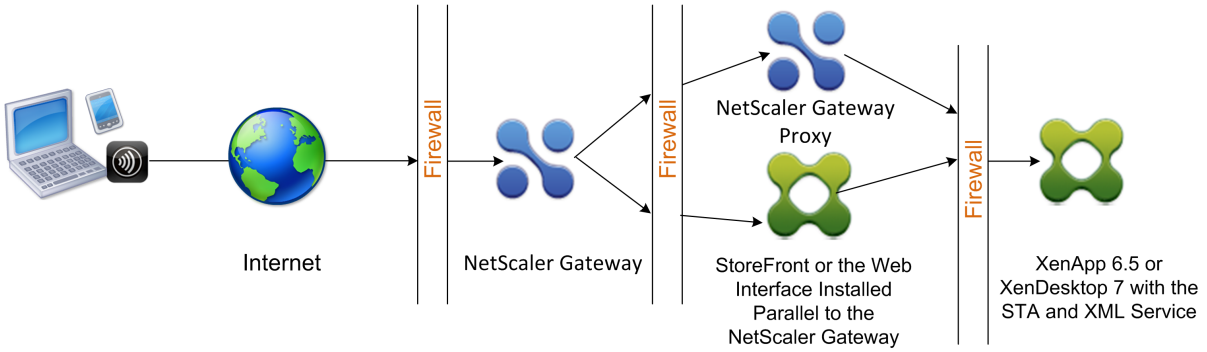
Después de reiniciar NetScaler Gateway, para comprobar que la instalación se ha realizado correctamente, inicie la utilidad de configuración. La versión de NetScaler Gateway que se encuentra en el dispositivo aparece en la esquina superior derecha.

Implementación de NetScaler Gateway en una DMZ de doble salto

March 27, 2024

Algunas empresas usan tres firewalls para proteger sus redes internas. Esos tres firewalls dividen la zona desmilitarizada en dos niveles para ofrecer una capa extra de seguridad a la red interna. Esa configuración de red se llama “zona desmilitarizada de doble salto”.

Figura 1. Dispositivos NetScaler Gateway implementados en una DMZ de doble salto



> **Nota:**
>
> Con fines ilustrativos, el ejemplo anterior describe una configuración de doble salto que utiliza tres firewalls con StoreFront, la Interfaz Web y Citrix Virtual Apps. Sin embargo, también puede tener una DMZ de doble salto con un dispositivo en la DMZ y un dispositivo en la red segura. Si configura una configuración de doble salto con un dispositivo en la DMZ y otro en la red segura, puede ignorar las instrucciones para abrir puertos en el tercer firewall.

Puede configurar una DMZ de doble salto para admitir Citrix StoreFront o la Interfaz Web instalada en paralelo al proxy de NetScaler Gateway. Los usuarios se conectan mediante la aplicación Citrix Workspace.

> **Nota:**
>
> Si implementa NetScaler Gateway en una DMZ de doble salto con StoreFront, la aplicación AutoDiscovery para Citrix Workspace basada en correo electrónico no funciona.

Cómo funciona una implementación de doble salto

Puede implementar dispositivos NetScaler Gateway en una DMZ de doble salto para controlar el acceso a los servidores que ejecutan Citrix Virtual Apps. Las conexiones de una implementación de doble salto se producen de la siguiente manera:

- Los usuarios se conectan a NetScaler Gateway en la primera DMZ mediante un explorador web y mediante la aplicación Citrix Workspace para seleccionar una aplicación publicada.
- La aplicación Citrix Workspace se inicia en el dispositivo del usuario. El usuario se conecta a NetScaler Gateway para acceder a la aplicación publicada que se ejecuta en la comunidad de servidores en la red segura.

  Nota: Secure Hub y el cliente Citrix Secure Access para Windows no se admiten en una implementación de DMZ de doble salto. Solo se utiliza la aplicación Citrix Workspace para las conexiones de usuario.

- NetScaler Gateway en la primera DMZ gestiona las conexiones de los usuarios y realiza las funciones de seguridad de una VPN SSL. Este NetScaler Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.
- NetScaler Gateway en la segunda DMZ funciona como dispositivo proxy de NetScaler Gateway. Este NetScaler Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores. Las comunicaciones entre NetScaler Gateway en la primera DMZ y Secure Ticket Authority (STA) en la red interna también se realizan mediante proxy a través de NetScaler Gateway en la segunda DMZ.

NetScaler Gateway admite conexiones IPv4 e IPv6. Puede utilizar la utilidad de configuración para configurar la dirección IPv6.

En la tabla siguiente se sugiere la compatibilidad con la implementación de doble salto para las distintas funciones ICA:

Función ICA	Soporte de doble salto
SmartAccess	Sí
SmartControl	Sí
Enlightened Data Transport (EDT)	Sí
HDX Insight	Sí
Fiabilidad de la sesión ICA (puerto 2598)	Sí
Migración de sesiones ICA	Sí
Tiempo de espera de sesión ICA	Sí
ICA de multisecuencia	Sí (solo TCP)
Framehawk	No
Audio UDP	No

Prepárese para una implementación DMZ de doble salto

Al configurar una implementación de DMZ de doble salto, debe responder a las siguientes preguntas:

- ¿Quiero admitir el equilibrio de cargas?
- ¿Qué puertos se abren en los firewalls?
- ¿Cuántos certificados SSL necesito?
- ¿Qué componentes necesito antes de comenzar la implementación?

Los temas de esta sección contienen información que le ayudará a responder a estas preguntas según corresponda a su entorno.

Componentes necesarios para iniciar la implementación

Antes de comenzar una implementación de DMZ de doble salto, asegúrese de que dispone de los siguientes componentes:

- Como mínimo, deben estar disponibles dos dispositivos NetScaler Gateway (uno para cada DMZ).
- Los servidores que ejecutan Citrix Virtual Apps deben estar instalados y operativos en la red interna.
- La Interfaz Web o StoreFront deben instalarse en la segunda DMZ y configurarse para funcionar con el conjunto de servidores de la red interna.
- Como mínimo, se debe instalar un certificado de servidor SSL en NetScaler Gateway en la primera DMZ. Este certificado garantiza que el explorador web y las conexiones de usuario a NetScaler Gateway estén cifradas.

  Necesita certificados adicionales si quiere cifrar las conexiones que se producen entre los demás componentes de una implementación DMZ de doble salto.

Flujo de comunicación en una implementación DMZ de doble salto

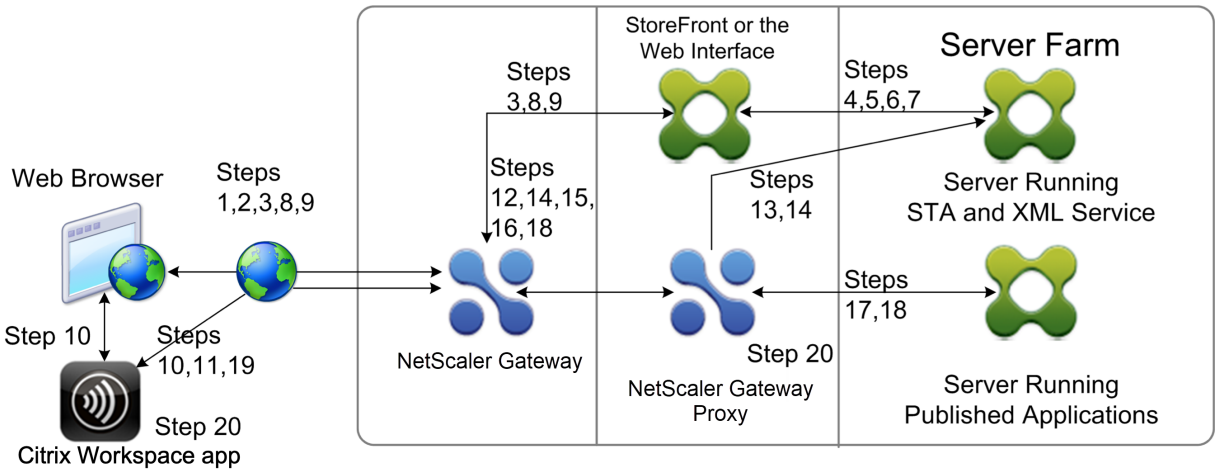
January 26, 2024

Para comprender los problemas de configuración relacionados con una implementación DMZ de doble salto, debe tener conocimientos básicos de cómo se comunican los distintos componentes de NetScaler Gateway y Citrix Virtual Apps de una implementación DMZ de doble salto para admitir una conexión de usuario. El proceso de conexión de StoreFront y la interfaz web es el mismo.

Aunque el proceso de conexión de usuario se produce en un flujo continuo, los siguientes pasos de alto nivel están implicados en el proceso.

- Autenticar usuarios
- Crear un tíquet de sesión
- Inicie la aplicación Citrix Workspace
- Completa la conexión

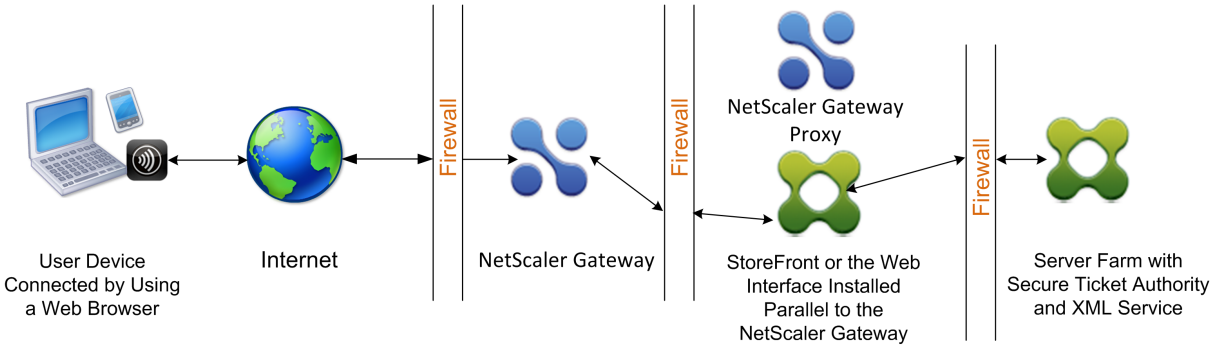
En la siguiente ilustración se muestran los pasos que se producen en el proceso de conexión del usuario a StoreFront o a la interfaz web. En la red segura, los equipos que ejecutan Citrix Virtual Apps también ejecutan Secure Ticket Authority (STA), XML Service y aplicaciones publicadas.



Proceso de conexión

La autenticación de usuarios es el primer paso del proceso de conexión de usuarios en una implementación DMZ de doble salto.

En la siguiente ilustración se muestra el proceso de conexión de usuarios de esta implementación.



Durante la fase de autenticación de usuarios, se produce el siguiente proceso básico:

1. Un usuario escribe la dirección de NetScaler Gateway, por ejemplo, https://www.ng.wxyco.com, en un explorador web para conectarse a NetScaler Gateway en la primera DMZ. Si ha habilitado la autenticación de la página de inicio de sesión en NetScaler Gateway, NetScaler Gateway autentica al usuario.
2. NetScaler Gateway en la primera DMZ recibe la solicitud.
3. NetScaler Gateway redirige la conexión del explorador web a la interfaz web.
4. La interfaz web envía las credenciales de usuario al servicio Citrix XML que se ejecuta en el conjunto de servidores de la red interna.

5. Citrix XML Service autentica al usuario.
6. El servicio XML crea una lista de las aplicaciones publicadas a las que el usuario tiene autorización para acceder y envía esta lista a la interfaz web.

   Nota:

   - Si habilita la autenticación en NetScaler Gateway, el dispositivo envía la página de inicio de sesión de NetScaler Gateway al usuario. El usuario introduce las credenciales de autenticación en la página de inicio de sesión y el dispositivo autentica al usuario. A continuación, NetScaler Gateway devuelve las credenciales de usuario a la interfaz web.
   - Si no habilita la autenticación, NetScaler Gateway no realiza la autenticación. El dispositivo se conecta a la interfaz web, recupera la página de inicio de sesión de la interfaz web y envía la página de inicio de sesión de la interfaz web al usuario. El usuario introduce las credenciales de autenticación en la página de inicio de sesión de la Interfaz Web y NetScaler Gateway devuelve las credenciales de usuario a la interfaz web.

   La creación del tíquet de sesión es la segunda etapa del proceso de conexión de usuario en una implementación DMZ de doble salto.

   Durante la etapa de creación del tíquet de sesión, se produce el siguiente proceso básico:

7. La interfaz web se comunica tanto con el servicio XML como con la Secure Ticket Authority (STA) de la red interna para producir tíquets de sesión para cada una de las aplicaciones publicadas a las que el usuario tiene autorización para acceder. El vale de sesión contiene una dirección de alias para el equipo que ejecuta Citrix Virtual Apps que aloja una aplicación publicada.
8. El STA guarda las direcciones IP de los servidores que alojan las aplicaciones publicadas. A continuación, el STA envía los tíquets de sesión solicitados a la interfaz web. Cada vale de sesión incluye un alias que representa la dirección IP del servidor que aloja la aplicación publicada, pero no la dirección IP real.
9. La interfaz web genera un archivo ICA para cada una de las aplicaciones publicadas. El archivo ICA contiene el tíquet emitido por la STA. A continuación, la interfaz web crea y rellena una página web con una lista de vínculos a las aplicaciones publicadas y envía esta página web al explorador web del dispositivo del usuario.

   El inicio de la aplicación Citrix Workspace es la tercera etapa del proceso de conexión de usuario en una implementación DMZ de doble salto. El proceso básico es el siguiente:

10. El usuario hace clic en un enlace a una aplicación publicada en la interfaz web. La interfaz web envía el archivo ICA de esa aplicación publicada al explorador del dispositivo del usuario.

    El archivo ICA contiene datos que indican al explorador web que inicie Receiver.

    El archivo ICA también contiene el nombre de dominio completo (FQDN) o el nombre del sistema de nombres de dominio (DNS) de NetScaler Gateway en la primera DMZ.

11. El explorador web inicia Receiver y el usuario se conecta a NetScaler Gateway en la primera DMZ mediante el nombre de NetScaler Gateway del archivo ICA. El enlace inicial de SSL/TLS se produce para establecer la identidad del servidor que ejecuta NetScaler Gateway.

    La finalización de la conexión es la cuarta y última etapa del proceso de conexión de usuario en una implementación DMZ de doble salto.

    Durante la fase de finalización de la conexión, se produce el siguiente proceso básico:

    - El usuario hace clic en un enlace a una aplicación publicada en la interfaz web.
    - El explorador web recibe el archivo ICA generado por la interfaz web e inicia la aplicación Citrix Workspace.
      Nota: El archivo ICA contiene código que indica al explorador web que inicie la aplicación Citrix Workspace.
    - La aplicación Citrix Workspace inicia una conexión ICA con NetScaler Gateway en la primera DMZ.
    - NetScaler Gateway en la primera DMZ se comunica con Secure Ticket Authority (STA) de la red interna para resolver la dirección de alias del tíquet de sesión en la dirección IP real de un equipo que ejecuta Citrix Virtual Apps o StoreFront. Esta comunicación se transforma mediante proxy a través de la segunda DMZ por el proxy de NetScaler Gateway.
    - NetScaler Gateway en la primera DMZ completa la conexión ICA a la aplicación Citrix Workspace.
    - La aplicación Citrix Workspace ahora se puede comunicar a través de ambos dispositivos NetScaler Gateway con el equipo que ejecuta Citrix Virtual Apps en la red interna.

    Los pasos detallados para completar el proceso de conexión de usuario son los siguientes:

12. La aplicación Citrix Workspace envía el tíquet STA de la aplicación publicada a NetScaler Gateway en la primera DMZ.

13. NetScaler Gateway en la primera DMZ se pone en contacto con el STA de la red interna para validar los tíquets. Para ponerse en contacto con STA, NetScaler Gateway establece un SOCKS o SOCKS con conexión SSL al proxy de NetScaler Gateway en la segunda DMZ.

14. El proxy de NetScaler Gateway de la segunda DMZ transfiere la solicitud de validación de tíquets al STA de la red interna. STA valida el tíquet y lo asigna al equipo que ejecuta Citrix Virtual Apps que aloja la aplicación publicada.

15. El STA envía una respuesta al proxy de NetScaler Gateway en la segunda DMZ, que se transfiere a NetScaler Gateway en la primera DMZ. Esta respuesta completa la validación del tíquet e incluye la dirección IP del equipo que aloja la aplicación publicada.

16. NetScaler Gateway en la primera DMZ incorpora la dirección del servidor Citrix Virtual Apps en el paquete de conexión de usuario y envía este paquete al proxy de NetScaler Gateway en la segunda DMZ.

17. El proxy de NetScaler Gateway de la segunda DMZ realiza una solicitud de conexión al servidor especificado en el paquete de conexión.
18. El servidor responde al proxy de NetScaler Gateway en la segunda DMZ. El proxy de NetScaler Gateway de la segunda DMZ transfiere esta respuesta a NetScaler Gateway en la primera DMZ para completar la conexión entre el servidor y NetScaler Gateway en la primera DMZ.
19. NetScaler Gateway en la primera DMZ completa el enlace SSL/TLS con el dispositivo del usuario transmitiendo el paquete de conexión final al dispositivo del usuario. Se establece la conexión del dispositivo del usuario al servidor.
20. El tráfico ICA fluye entre el dispositivo de usuario y el servidor a través de NetScaler Gateway en la primera DMZ y el proxy de NetScaler Gateway en la segunda DMZ.

Instalación y configuración de NetScaler Gateway en una DMZ de doble salto

March 27, 2024

Debe completar varios pasos para implementar NetScaler Gateway en una DMZ de doble salto. Los pasos incluyen la instalación de dispositivos en ambas DMZ y la configuración de los dispositivos para las conexiones de dispositivos de usuario.

Instale NetScaler Gateway en la primera DMZ

Para instalar NetScaler Gateway en la primera DMZ, siga las instrucciones de Instalación del hardware.

Si va a instalar varios dispositivos NetScaler Gateway en la primera DMZ, puede implementar los dispositivos detrás de un equilibrador de carga.

Configurar NetScaler Gateway en la primera DMZ

En una implementación de DMZ de doble salto, es obligatorio configurar cada NetScaler Gateway de la primera DMZ para redirigir las conexiones a StoreFront o a la interfaz web de la segunda DMZ.

La redirección a StoreFront o a la interfaz web se realiza a nivel de servidor virtual o global de NetScaler Gateway. Para conectarse a la interfaz web a través de NetScaler Gateway, un usuario debe estar asociado a un grupo de usuarios de NetScaler Gateway para el que esté habilitada la redirección a la interfaz web.

Instale NetScaler Gateway en la segunda DMZ

El dispositivo NetScaler Gateway de la segunda DMZ se denomina proxy de NetScaler Gateway porque dirige el tráfico ICA y Secure Ticket Authority (STA) a través de la segunda DMZ.
Instale el hardware para instalar cada dispositivo NetScaler Gateway en la segunda DMZ.

Puede utilizar este procedimiento de instalación para instalar otros dispositivos en la segunda DMZ.

Después de instalar los dispositivos NetScaler Gateway en la segunda DMZ, configure los siguientes valores:

- Configure un servidor virtual en el proxy de NetScaler Gateway.
- Configure los dispositivos NetScaler Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlazar NetScaler Gateway en la segunda DMZ de forma global o a un servidor virtual.
- Configure STA en el dispositivo de la primera zona desmilitarizada.
- Abra los puertos de los firewalls que separan la zona desmilitarizada.
- Instale certificados en los dispositivos.

Configurar los ajustes en los servidores virtuales del proxy de NetScaler Gateway

January 26, 2024

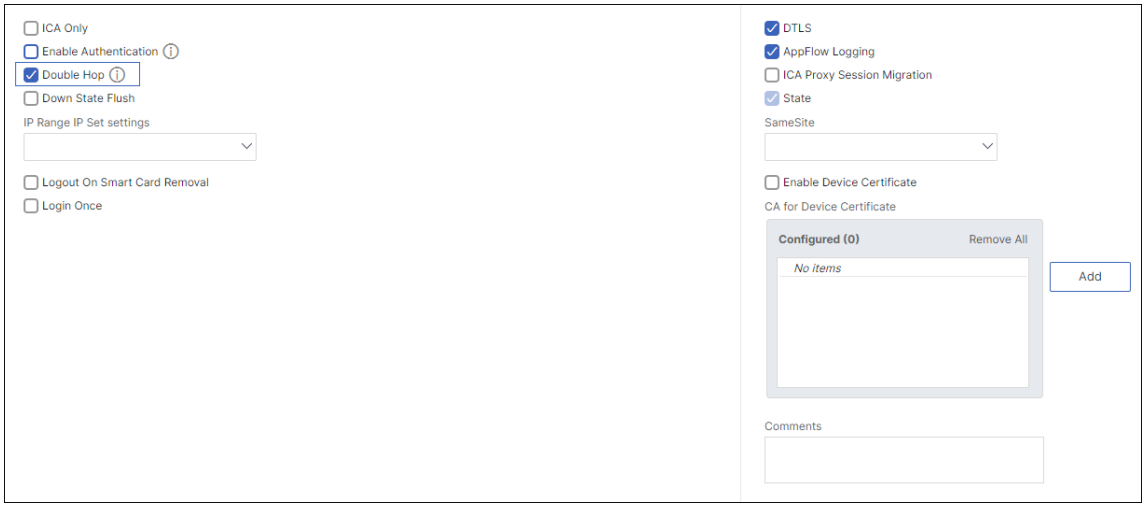
Para permitir el paso de conexiones entre los dispositivos NetScaler Gateway, habilite el doble salto en el servidor virtual del proxy NetScaler Gateway.

Cuando los usuarios se conectan, el dispositivo NetScaler Gateway autentica a los usuarios y, a continuación, envía como proxy la conexión al dispositivo proxy. En NetScaler Gateway en la primera DMZ, configure el servidor virtual para que se comunique con NetScaler Gateway en la segunda DMZ. No configure la autenticación ni las directivas en el proxy de NetScaler Gateway. Citrix recomienda inhabilitar la autenticación en el servidor virtual.

Para habilitar el doble salto en el servidor virtual del proxy de NetScaler Gateway mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En la sección **Configuración básica**, haga clic en el icono de modificación y, a continuación, haga clic en **Más**.

4. Selecciona **Doble salto**.

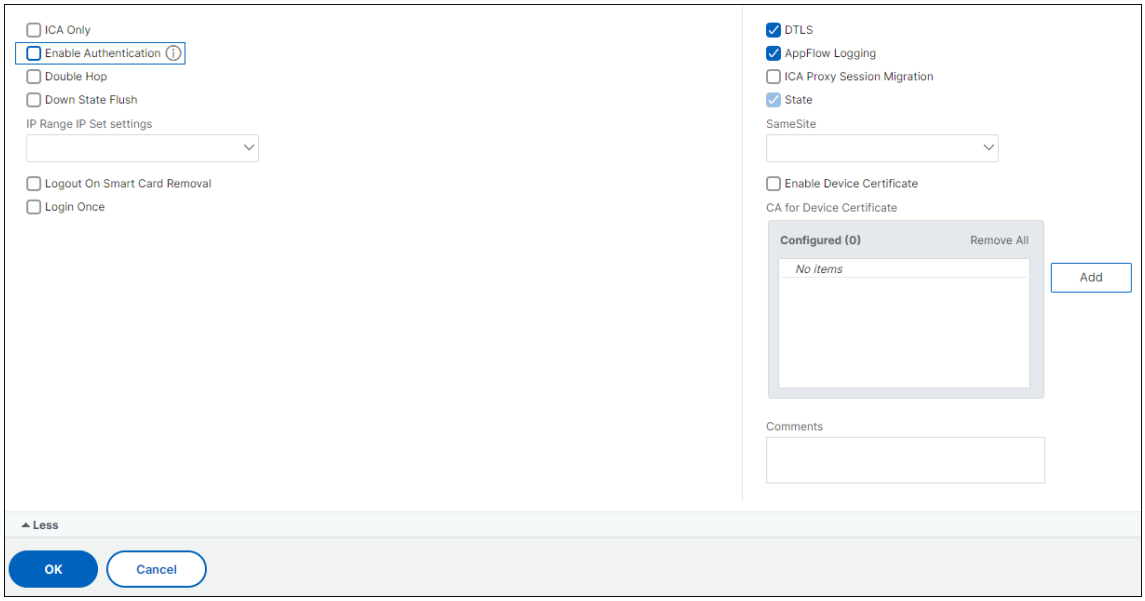


5. Haga clic en **Aceptar**.

Para inhabilitar la autenticación en el servidor virtual del proxy de NetScaler Gateway mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. En la sección **Configuración básica**, haga clic en el icono de modificación y, a continuación, haga clic en **Más**.

4. Desactive la casilla de verificación **Habilitar autenticación**.



5. Haga clic en **Aceptar**.

Configurar el dispositivo para que se comunique con el proxy del dispositivo

March 27, 2024

Al implementar NetScaler Gateway en una DMZ de doble salto, debe configurar NetScaler Gateway en la primera DMZ para que se comunique con el proxy de NetScaler Gateway en la segunda DMZ.

Si implementa varios dispositivos en la segunda DMZ, configura cada dispositivo de la primera DMZ para que se comunique con todos los dispositivos proxy de la segunda DMZ.

Nota: Si quiere utilizar IPv6, configure el servidor de salto siguiente mediante la utilidad de configuración. Para ello, expanda
NetScaler Gateway > Recursos y, a continuación, haga clic en Servidores de
siguiente salto. Siga los pasos del procedimiento siguiente y, a continuación, active la casilla de verificación
IPv6.

Para configurar NetScaler Gateway para que se comunique con el proxy de NetScaler Gateway

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway > Recursos y, a continuación, haga clic en Servidores de salto siguiente.

2. En el panel de detalles, haga clic en Agregar.
3. En Nombre, escriba un nombre para el primer NetScaler Gateway.
4. En Dirección IP, escriba la dirección IP del servidor virtual del proxy de NetScaler Gateway en la segunda DMZ.
5. En Puerto, escriba el número de puerto, haga clic en Crear y, a continuación, haga clic en Cerrar. Si utiliza un puerto seguro, como el 443, seleccione Seguro.

Debe configurar cada NetScaler Gateway instalado en la primera DMZ para que se comunique con todos los dispositivos proxy de NetScaler Gateway instalados en la segunda DMZ.

Después de configurar la configuración del proxy de NetScaler Gateway, vincule la directiva a los servidores Next Hop de NetScaler Gateway Global o a un servidor virtual.

Para enlazar el servidor de siguiente salto de NetScaler Gateway de forma global

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway > Recursos y, a continuación, haga clic en Servidores de salto siguiente.
2. En el panel de detalles, seleccione un servidor de salto siguiente y, a continuación, en Acción, seleccione Enlaces globales.
3. En el cuadro de diálogo Configurar enlace global del servidor de salto siguiente, en Nombre del servidor de salto siguiente, seleccione el dispositivo proxy y, a continuación, haga clic en Aceptar.

Para enlazar el servidor de siguiente salto de NetScaler Gateway a un servidor virtual

1. En la utilidad de configuración, en la ficha Configuración, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la ficha Aplicaciones publicadas, en Servidores Next Hop, haga clic en un elemento y, a continuación, haga clic en Aceptar.

También puede agregar un servidor de siguiente salto desde la ficha Aplicaciones publicadas.

Configurar NetScaler Gateway para gestionar el tráfico de STA e ICA

March 27, 2024

Al implementar NetScaler Gateway en una DMZ de doble salto, debe configurar NetScaler Gateway en la primera DMZ para gestionar las comunicaciones con Secure Ticket Authority (STA) y el tráfico

ICA de forma adecuada. El servidor que ejecuta STA se puede enlazar de forma global o a un servidor virtual.

Después de configurar el STA, puede enlazar el STA de forma global o a un servidor virtual.

Para configurar y enlazar el STA de forma global:

1. En la GUI, en la ficha Configuración, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Servidores**, haga clic en **Vincular o desvincular los servidores STA que utilizará Secure Ticket Authority**.
3. En el cuadro de diálogo **Enlazar/desenlazar servidores STA**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Configurar servidor STA** , en **URL** , escriba la ruta al servidor que ejecuta STA, como o http://mycompany.comhttp://ipAddressy, a continuación, haga clic en **Crear** .

Para configurar y enlazar el STA a un servidor virtual:

1. En la GUI, en la ficha Configuración, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en **Abrir** .
3. En la pestaña **Aplicaciones publicadas** , en **Secure Ticket Authority** , haga clic en **Agregar** .
4. En el cuadro de diálogo **Configurar servidor STA**, en URL, escriba la ruta al servidor que ejecuta STA, como http://mycompany.com o http://ipAddress y, a continuación, haga clic en **Crear**.

Nota:

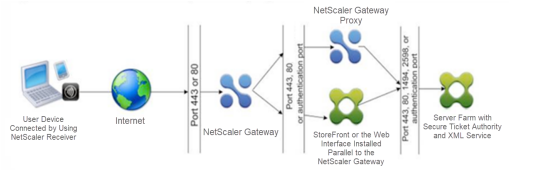
Si los servidores virtuales VPN comparten el mismo servidor virtual de siguiente salto y servidores STA, la conexión se restablece cuando el servidor STA común se desvincula de un servidor virtual que comparte el mismo servidor virtual de siguiente salto.

Abra los puertos apropiados en los firewalls

January 26, 2024

Debe asegurarse de que los puertos adecuados estén abiertos en los firewalls para admitir las distintas conexiones que se producen entre los distintos componentes implicados en una implementación de DMZ de doble salto. Para obtener más información sobre el proceso de conexión, consulte Flujo de comunicación en una implementación DMZ de doble salto.

En la siguiente ilustración se muestran los puertos comunes que se pueden utilizar en una implementación DMZ de doble salto.



En la tabla siguiente se muestran las conexiones que se producen a través del primer firewall y los puertos que deben estar abiertos para admitir las conexiones.

Conexiones a través del primer firewall	Puertos utilizados
El explorador web de Internet se conecta a NetScaler Gateway en la primera DMZ. **Nota:** NetScaler Gateway incluye una opción para redirigir las conexiones realizadas en el puerto 80 a un puerto seguro. Si habilita esta opción en NetScaler Gateway, puede abrir el puerto 80 a través del primer firewall. Cuando un usuario establece una conexión sin cifrar a NetScaler Gateway en el puerto 80, NetScaler Gateway redirige automáticamente la conexión a un puerto seguro.	Abra el puerto TCP 443 a través del primer firewall.
La aplicación Citrix Workspace desde Internet se conecta a NetScaler Gateway en la primera DMZ.	Abra el puerto TCP 443 a través del primer firewall.

En la tabla siguiente se muestran las conexiones que se producen a través del segundo firewall y los puertos que deben estar abiertos para admitir las conexiones.

Conexiones a través del segundo firewall	Puertos utilizados
NetScaler Gateway en la primera DMZ se conecta a la interfaz web en la segunda DMZ.	Abra el puerto TCP 80 para una conexión no segura o el puerto TCP 443 para una conexión segura a través del segundo firewall.
NetScaler Gateway en la primera DMZ se conecta a NetScaler Gateway en la segunda DMZ.	Abra el puerto TCP 443 para obtener una conexión SOCKS segura a través del segundo firewall.
Si ha habilitado la autenticación en NetScaler Gateway en la primera DMZ, es posible que este dispositivo deba conectarse a un servidor de autenticación de la red interna.	Abra el puerto TCP en el que el servidor de autenticación escucha las conexiones. Los ejemplos incluyen el puerto 1812 para RADIUS y el puerto 389 para LDAP.

En la tabla siguiente se muestran las conexiones que se producen a través del tercer firewall y los puertos que deben estar abiertos para admitir las conexiones.

Conexiones a través del tercer firewall	Puertos utilizados
StoreFront o la interfaz web de la segunda DMZ se conectan al servicio XML alojado en un servidor de la red interna.	Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall.
StoreFront o la interfaz web de la segunda DMZ se conectan a la Secure Ticket Authority (STA) alojada en un servidor de la red interna.	Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall.
NetScaler Gateway en la segunda DMZ se conecta al STA que reside en la red segura.	Abra el puerto 80 para una conexión no segura o el puerto 443 para una conexión segura a través del tercer firewall.
NetScaler Gateway en la segunda DMZ establece una conexión ICA con una aplicación publicada o un escritorio virtual en un servidor de la red interna.	Abra el puerto TCP 1494 para admitir conexiones ICA a través del tercer firewall. Si ha habilitado la fiabilidad de la sesión en Citrix Virtual Apps, abra el puerto TCP 2598 en lugar del 1494.
Si ha habilitado la autenticación en NetScaler Gateway en la primera DMZ, es posible que este dispositivo deba conectarse a un servidor de autenticación de la red interna.	Abra el puerto TCP en el que el servidor de autenticación escucha las conexiones. Los ejemplos incluyen el puerto 1812 para RADIUS y el puerto 389 para LDAP.

Mantener y supervisar el sistema

January 26, 2024

Una vez que haya completado la configuración de su NetScaler Gateway, deberá mantener y supervisar el dispositivo. Puede hacerlo de las siguientes maneras:

- Puede actualizar NetScaler Gateway a la versión más reciente del software. Al iniciar sesión en el sitio web de Citrix, puede ir al sitio de descargas de NetScaler Gateway y descargar el software. Puede encontrar el archivo léame de las compilaciones de mantenimiento en Citrix Knowledge Center.
- Puede asignar tareas de configuración y administración de NetScaler Gateway a distintos miembros del grupo. Con la administración delegada, puede asignar niveles de acceso a personas que les limitan a realizar tareas específicas en NetScaler Gateway.

- Puede guardar la configuración de NetScaler Gateway en el dispositivo o en un archivo del equipo. Puede comparar la configuración actual en ejecución y la configuración guardada. También puede borrar la configuración de NetScaler Gateway.
- Puede ver, actualizar y sesiones de usuario final en la utilidad de configuración de NetScaler Gateway.
- Puede configurar el registro en NetScaler Gateway. Los registros proporcionan información importante sobre el dispositivo y son útiles en caso de que se produzcan problemas.

Configurar administradores delegados

January 26, 2024

NetScaler Gateway tiene un nombre de usuario y una contraseña de administrador predeterminados. El nombre de usuario y la contraseña predeterminados son `nsroot`. Al ejecutar el Asistente de configuración por primera vez, puede cambiar la contraseña de administrador.

Puede crear más cuentas de administrador y asignar a cada cuenta distintos niveles de acceso a NetScaler Gateway. Estas cuentas adicionales se denominan administradores delegados. Por ejemplo, tiene una persona asignada para supervisar las conexiones y los registros de NetScaler Gateway y otra persona responsable de configurar valores específicos en NetScaler Gateway. El primer administrador tiene acceso de solo lectura y el segundo administrador tiene acceso limitado al dispositivo.

Para configurar un administrador delegado, utilice directivas de comandos y usuarios y grupos del sistema.

Al configurar un administrador delegado, el proceso de configuración es:

- Agregue un usuario del sistema. Un usuario del sistema es un administrador con los privilegios especificados. Todos los administradores heredan las directivas de los grupos a los que pertenecen.
- Agregue un grupo de sistemas. Un grupo de sistemas contiene usuarios de sistemas con privilegios específicos. Los miembros del grupo del sistema heredan las directivas del grupo o grupos a los que pertenecen.
- Cree una directiva de comandos. Las directivas de comandos permiten definir qué partes de la configuración de NetScaler Gateway pueden acceder y modificar un usuario o un grupo. También puede regular qué comandos, como grupos de comandos, servidores virtuales y otros elementos que los administradores y grupos pueden configurar.
- Enlazar la directiva de comandos al usuario o grupo estableciendo la prioridad. Al configurar la administración delegada, asigne prioridades al administrador o al grupo para que NetScaler Gateway pueda determinar qué directiva tiene prioridad.

NetScaler Gateway tiene una directiva de comandos de deny system predeterminada. Las directivas de comandos no se pueden enlazar globalmente. Enlazar las directivas directamente a los administradores del sistema (usuarios) o grupos. Si los usuarios y los grupos no tienen una directiva de comandos asociada, se aplica la directiva de denegación predeterminada y los usuarios no pueden ejecutar ningún comando ni configurar NetScaler Gateway.

Puede configurar directivas de comandos personalizadas para definir un mayor nivel de detalle para las asignaciones de derechos de usuario. Por ejemplo, puede dar a una persona la posibilidad de agregar directivas de sesión a NetScaler Gateway, pero no permitir que el usuario realice ninguna otra configuración.

Configurar directivas de comandos para administradores delegados

January 26, 2024

NetScaler Gateway tiene cuatro directivas de comandos integradas que puede utilizar para la administración delegada:

- **Solo lectura** permite el acceso de solo lectura para mostrar todos los comandos excepto el grupo de comandos del sistema y comandos `ns.conf show`.
- El**operador** permite el acceso de solo lectura y también permite el acceso para habilitar y inhabilitar comandos en los servicios. Esta directiva también permite el acceso para establecer servicios y servidores como "acceso inactivo".
- La**red** permite un acceso casi completo al sistema, excluyendo los comandos del sistema y el comando shell.
- El **superusuario** concede todos los privilegios del sistema, como los privilegios concedidos al administrador predeterminado `nsroot`.

Las directivas de comandos contienen expresiones integradas. Utilice la utilidad de configuración para crear usuarios del sistema, grupos de sistemas, directivas de comandos y definir permisos.

Para crear un usuario administrativo en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Usuarios del sistema**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de usuario**, escriba un nombre de usuario.
4. En los campos **Contraseña** y **Confirmar contraseña**, escriba la contraseña.
5. Para agregar usuarios a un grupo, en **Miembro de**, haga clic en **Agregar**.
6. En **Disponible**, seleccione un grupo y, a continuación, haga clic en la flecha derecha.

7. Haga clic en **Directivas de comandos > Acción > Insertar**.
8. En el cuadro de diálogo Insertar directivas de comandos, seleccione el comando y haga clic en **Aceptar > Crear > Cerrar**.

Creación de grupos administrativos

Los grupos administrativos contienen usuarios con privilegios administrativos en NetScaler Gateway. Puede crear grupos administrativos en la utilidad de configuración.

Para configurar un grupo administrativo mediante la utilidad de configuración

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Grupos de sistemas**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo**, escriba un nombre para el grupo.
4. Para agregar un usuario existente al grupo, en **Miembros**, haga clic en **Agregar**.
5. En **Disponible**, seleccione un usuario y, a continuación, haga clic en la flecha derecha.
6. En **Directivas de comandos**, en **Acción**, haga clic en **Insertar**, seleccione una directiva o directivas, haga clic en **Aceptar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Configurar directivas de comandos personalizadas para administradores delegados

March 27, 2024

Al configurar una directiva de comandos personalizada, se proporciona un nombre de directiva y, a continuación, se configuran los componentes de la directiva para crear la especificación de comandos. Con la especificación de comandos, puede limitar los comandos que pueden usar los administradores. Por ejemplo, quiere denegar a los administradores la posibilidad de utilizar el comando remove. Al configurar la directiva, defina la acción en denegar y, a continuación, configure los parámetros.

Puede configurar una directiva de comandos sencilla o avanzada. Al configurar una directiva sencilla, configura un componente en el dispositivo, como NetScaler Gateway y la autenticación. Al configurar una directiva avanzada, selecciona el componente, denominado grupo de entidades y, a continuación, selecciona los comandos que los administradores pueden ejecutar en el grupo.

Para crear una directiva de comandos personalizada sencilla

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema** > **Administración de usuario** y, a continuación, haga clic en **Directivas de comando.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre de la directiva**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Especificación de comandos**, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar comando**, en la ficha **Simple**, en Operación, seleccione la acción que pueden realizar los administradores delegados.
7. En **Grupo de entidades**, seleccione uno o varios grupos.

   Puede presionar la tecla CTRL para seleccionar varios grupos.
8. Haga clic en **Create** y, luego, en **Close**.

Para crear una directiva de comandos personalizada avanzada

1. En la utilidad de configuración, en el panel de navegación, en la ficha **Configuración**, expanda **Sistema** > **Administración de usuario** y, a continuación, haga clic en **Directivas de comando**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de la directiva**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Especificación de comandos**, haga clic en **Agregar**.
6. En el cuadro de diálogo **Agregar comando**, haga clic en la ficha **Avanzadas**.
7. En **Grupo de entidades**, seleccione el grupo al que pertenece el comando, como autenticación o alta disponibilidad.
8. En **Entidad**, seleccione la directiva.

   Puede presionar la tecla CTRL para seleccionar varios elementos de la lista.
9. En **Operación**, seleccione el comando, haga clic en **Crear y,** a continuación, haga clic en **Cerrar**.

   Puede presionar la tecla CTRL para seleccionar varios elementos de la lista.
10. Haga clic en **Crear** y, a continuación, en **Cerrar**.
11. En el cuadro de diálogo **Crear directiva de comandos**, haga clic en **Crear y,** a continuación, en **Cerrar**.

Al hacer clic en **Crear**, la expresión aparece en Especificaciones de comandos en el cuadro de diálogo **Crear directiva de comandos** .

Después de crear la directiva de comandos personalizada, puede vincularla a un usuario o a un grupo.

> **Nota:** Solo puede enlazar directivas de comandos personalizadas a los usuarios o grupos que cree. No se puede enlazar una directiva de comandos personalizada al usuario `nsroot`.

Para enlazar una directiva de comandos personalizada a un usuario o grupo

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema** > **Administración de usuarios** y, a continuación, haga clic en **Usuarios del sistema** o en **Grupos de sistemas**.
2. En el panel de detalles, seleccione un usuario o grupo de la lista y, a continuación, haga clic en **Abrir**.
3. En **Directivas de comandos**, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

Configurar la auditoría en NetScaler Gateway

January 26, 2024

NetScaler Gateway permite registrar los estados y la información de estado que recopila el dispositivo. Puede utilizar los registros de auditoría para ver el historial de sucesos en orden cronológico. Los mensajes de los registros contienen información sobre el suceso que generó el mensaje, una marca de tiempo, el tipo de mensaje y niveles de registro predefinidos e información del mensaje. Puede configurar ajustes que determinan la información que se registra y la ubicación en la que se almacenan los mensajes.

NetScaler Gateway admite actualmente dos formatos de registro: un formato de registro propietario para registros locales y el formato syslog para usar con servidores syslog. Puede configurar los registros de auditoría para que proporcionen la siguiente información:

Nivel	Descripción
EMERGENCIA	Registra solo los errores principales. Las entradas del registro indican que NetScaler Gateway está experimentando un problema crítico que hace que no se pueda utilizar.

Nivel	Descripción
ALERTA	Registra problemas que pueden hacer que NetScaler Gateway funcione incorrectamente, pero que no son críticos para su funcionamiento. Se pueden tomar medidas correctivas lo antes posible para evitar que NetScaler Gateway experimente un problema crítico.
CRÍTICO	Registra las condiciones críticas que no restringen el funcionamiento de NetScaler Gateway, pero que pueden derivar a un problema mayor.
ERROR	Registra las entradas resultantes de una operación fallida en NetScaler Gateway.
ADVERTENCIA	Registra posibles problemas que pueden dar lugar a un error o a un error crítico.
NOTIFICACIÓN	Registra problemas más detallados que el registro de nivel de información, pero tiene el mismo propósito que la notificación.
INFORMACIÓN	Registra las acciones realizadas por NetScaler Gateway. Este nivel es útil para solucionar problemas.

El registro de auditoría de NetScaler Gateway también almacena estadísticas de compresión de NetScaler Gateway si configura la compresión TCP. La relación de compresión alcanzada para los distintos datos se almacena en el archivo de registro de cada sesión de usuario.

NetScaler Gateway utiliza la firma de registro SessionID. Esto le permite realizar un seguimiento de los registros por sesión en lugar de por usuario. Los registros que se generan como parte de una sesión tienen el mismo SessionID. Si un usuario establece dos sesiones desde el mismo dispositivo de usuario con la misma dirección IP, cada sesión tiene un ID de sesión único.

> **Importante:** Si ha escrito scripts de análisis de registros personalizados, tendrá que cambiar esta firma dentro de los scripts de análisis personalizados.

Configurar registros en NetScaler Gateway

March 27, 2024

Al configurar el registro en NetScaler Gateway, puede elegir almacenar los registros de auditoría en NetScaler Gateway o enviarlos a un servidor syslog. La utilidad de configuración se utiliza para crear directivas de auditoría y configurar los ajustes para almacenar los registros de auditoría.

Para crear una directiva de auditoría

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. En **Nombre**, escriba un nombre para la directiva.
3. Seleccione una de estas opciones:
   - Syslog si quiere enviar los registros a un servidor Syslog.
   - `Nslog` para almacenar los registros en NetScaler Gateway.

     > **Nota:** Si selecciona esta opción, los registros se almacenan en la carpeta /var/log del dispositivo.
4. En el panel de detalles, haga clic en **Agregar**.
5. Escriba la siguiente información para la información del servidor en el que se almacenan los registros:
   - En Nombre, escriba el nombre del servidor.
   - En Servidor, escriba el nombre o la dirección IP del servidor de registros.
6. Haga clic en Crear y, a continuación, en Cerrar.

Después de crear la directiva de auditoría, puede vincularla a cualquier combinación de lo siguiente:

- Globalmente
- Servidores virtuales
- Grupos
- Usuarios

Para enlazar una directiva de auditoría de forma global

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione **`Syslog`** o **`Nslog`**.
3. En el panel de detalles, haga clic en **Acción** y, a continuación, haga clic en **Enlaces globales**.
4. En el cuadro de diálogo **Vincular o desvincular directivas de auditoría** a **global**, en **Detalles**, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, seleccione una directiva y, a continuación, haga clic en **Aceptar**.

Para modificar una directiva de auditoría

Puede modificar una directiva de auditoría existente para cambiar el servidor al que se envían los registros.

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**
2. Seleccione **Syslog** o **Nslog**.
3. En el panel de detalles, haga clic en una directiva y, a continuación, haga clic en **Abrir**.
4. En Servidor, seleccione el nuevo servidor y, a continuación, haga clic en **Aceptar**.

Para quitar una directiva de auditoría

Puede quitar una directiva de auditoría de NetScaler Gateway. Al quitar una directiva de auditoría, la directiva se desvinculará automáticamente.

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione **Syslog** o **Nslog**.
3. En el panel de detalles, haga clic en una directiva y, a continuación, en **Quitar**.

Configurar el registro de ACL

January 26, 2024

Puede configurar NetScaler Gateway para que registre los detalles de los paquetes que coinciden con una lista de control de acceso ampliado (ACL). Además del nombre de la ACL, los detalles registrados incluyen información específica del paquete, como las direcciones IP de origen y destino. La información se almacena en un syslog o en un archivo `nslog`, según el tipo de registro (syslog o `nslog`) que habilite.

Puede habilitar el registro tanto a nivel global como a nivel de ACL. Sin embargo, para habilitar el registro a nivel de ACL, también debe habilitarlo a nivel global. La configuración global tiene prioridad.

Para optimizar el registro, cuando varios paquetes del mismo flujo coinciden con una ACL, solo se registran los detalles del primer paquete. El contador se incrementa para todos los demás paquetes que pertenecen al mismo flujo. Un flujo se define como un conjunto de paquetes que tienen los mismos valores para los siguientes parámetros:

- IP de origen
- IP de destino

- Puerto de origen
- Puerto de destino
- Protocolo (TCP o UDP)

Si el paquete no procede del mismo flujo o si la duración del tiempo supera el tiempo medio, se crea un nuevo flujo. El tiempo medio es el tiempo durante el cual los paquetes del mismo flujo no generan mensajes adicionales (aunque el contador se incrementa).

> **Nota:** El número total de flujos diferentes que se pueden registrar en un momento dado está limitado a 10.000.

En la tabla siguiente se describen los parámetros con los que se puede configurar el registro de ACL a nivel de regla para las ACL extendidas.

Nombre del parámetro	Descripción
`Logstate`	Estado de la función de registro de la ACL. Valores posibles: HABILITADO y INHABILITADO. Predeterminado: DISABLED.
`Ratelimit`	Número de mensajes de registro que puede generar una ACL específica. Valor predeterminado: 100.

Para configurar el registro de ACL mediante la utilidad de configuración

Puede configurar el registro para una ACL y especificar el número de mensajes de registro que puede generar la regla.

1. En la utilidad de configuración, en el panel de navegación, expanda **Sistema** > **Red** y, a continuación, haga clic en ACL.
2. En el panel de detalles, haga clic en la ficha **ACL extendidas** y, a continuación, haga clic en Agregar.
3. En el cuadro de diálogo **Crear ACL extendida**, en Nombre, escriba un nombre para la directiva.
4. Active la casilla de verificación **Estado del registro**.
5. En el cuadro de texto **Límite de velocidad de registro**, escriba el límite de velocidad que quiere especificar para la regla y, a continuación, haga clic en **Crear**.

Después de configurar el registro de ACL, puede habilitarlo en NetScaler Gateway. Cree una directiva de auditoría y, a continuación, enlaza a un usuario, grupo, servidor virtual o de forma global.

Para habilitar el registro ACL o TCP en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** > **Auditoría**.
2. Seleccione syslog o `nslog`.
3. En la ficha **Servidores**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Crear servidor de auditoría**, en **Nombre**, escriba un nombre para el servidor y, a continuación, configure la configuración del servidor.
5. Haga clic en Registro **ACL o RegistroTCP**y, a continuación, haga clic en**Crear**.

Habilitación del registro de Citrix Secure Access

March 27, 2024

Puede configurar el cliente Citrix Secure Access para que registre todos los errores en los archivos de texto almacenados en el dispositivo del usuario. Los usuarios pueden configurar el cliente Citrix Secure Access para establecer el nivel de registro en el dispositivo del usuario para registrar las actividades específicas del usuario. Cuando los usuarios configuran el registro, el complemento crea los dos archivos siguientes en el dispositivo del usuario:

- hooklog<num>.txt, que registra los mensajes de intercepción que genera el cliente Citrix Secure Access.
- nssslvpn.txt, que enumera los errores del plug-in.

> **Nota:** Los archivos hooklog.txt no se eliminan automáticamente. Citrix recomienda eliminar los archivos periódicamente.

Los registros de usuario se encuentran en los siguientes directorios de Windows del dispositivo del usuario:

- Windows XP (todos los usuarios): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (para usuarios específicos): %SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (todos los usuarios): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (para usuarios específicos): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGE
- Windows 7 (todos los usuarios): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (para usuarios específicos): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8 (todos los usuarios): %SystemDrive%:\ProgramData\Citrix\AGEE

- Windows 8 (para usuarios específicos): %SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

Puede utilizar estos archivos de registro para solucionar problemas del cliente Citrix Secure Access. Los usuarios pueden enviar los archivos de registro por correo electrónico al soporte técnico.

En el cuadro de diálogo de configuración, los usuarios pueden establecer el nivel de registro del cliente Citrix Secure Access. Los niveles de registro son:

- Grabar mensajes de error
- Grabar mensajes de sucesos
- Registre las estadísticas del cliente Citrix Secure Access
- Registra todos los errores, mensajes de eventos y estadísticas

Para obtener más información sobre la función de registro del cliente Citrix Secure Access para Windows, consulte Recopilación de registros mejorada para el cliente de Windows.

Para supervisar las conexiones ICA

January 26, 2024

Puede supervisar las sesiones de usuario activas en la comunidad de servidores mediante el cuadro de diálogo Conexiones
ICA. Este cuadro de diálogo proporciona la siguiente información:

- Nombre de usuario de la persona que se conecta a la comunidad de servidores
- Nombre de dominio de la comunidad de servidores
- Dirección IP del dispositivo del usuario
- Número de puerto del dispositivo de usuario
- Dirección IP del servidor que ejecuta Citrix Virtual Apps and Desktops
- Número de puerto del servidor que ejecuta Citrix Virtual Apps and Desktops

1. Vaya a **Configuración > NetScaler Gateway**.
2. En la sección **Supervisar conexiones**, haga clic en **Conexiones ICA**.

Registros de sesiones ICA

El `ns.log` archivo imprime los registros de sesiones ICA en el siguiente formato:

```
May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT
    0-PPE-1 : default ICA Message 141327 0 :  "[Remote ip =
    10.10.99.86:514] [EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-
    c6333447a76] Received response from STA server {
 sta-server=10.11.40.222:80,type=ResponseData }
```



```
 "
<!--NeedCopy-->
```

A partir de la versión 13.1, compilación 50.x, se realizan las siguientes mejoras en los registros ICA:

- Muestra los tipos de conexión, como TCP, EDT, CGP y SOCKS.
- Muestra el identificador único universal (UUID) ICA.
- Todos los registros STA se muestran como registros de nivel de información.

Autenticación y autorización

January 26, 2024

NetScaler Gateway emplea un diseño de autenticación flexible que permite una amplia personalización de la autenticación de usuarios para NetScaler Gateway. Puede utilizar servidores de autenticación estándar del sector y configurar NetScaler Gateway para autenticar a los usuarios en los servidores. NetScaler Gateway también admite la autenticación basada en los atributos presentes en un certificado de cliente. La autenticación de NetScaler Gateway está diseñada para dar cabida a procedimientos de autenticación sencillos que utilizan un único origen para la autenticación de usuarios y procedimientos de autenticación en cascada más complejos que dependen de varios tipos de autenticación.

La autenticación de NetScaler Gateway incorpora autenticación local para la creación de usuarios y grupos locales. Este diseño se centra en el uso de directivas para controlar los procedimientos de autenticación que configura. Las directivas que cree se pueden aplicar a nivel de servidor virtual o global de NetScaler Gateway y se pueden utilizar para establecer los parámetros del servidor de autenticación de forma condicional en función de la red de origen del usuario.

Dado que las directivas están enlazadas de forma global o a un servidor virtual, también puede asignar prioridades a sus directivas para crear una cascada de varios servidores de autenticación como parte de la autenticación.

NetScaler Gateway incluye compatibilidad con los siguientes tipos de autenticación.

- Locales
- Protocolo ligero de acceso a directorios (LDAP)
- RADIUS
- SAML
- TACACS+
- Autenticación de certificado de cliente (incluida la autenticación con tarjeta inteligente)

NetScaler Gateway también es compatible con RSA SecurID, Gemalto Protiva y SafeWord. Se utiliza un servidor RADIUS para configurar estos tipos de autenticación.

Aunque la autenticación permite a los usuarios iniciar sesión en NetScaler Gateway y conectarse a la red interna, la autorización define los recursos de la red segura a los que tienen acceso los usuarios. La autorización se configura con directivas LDAP y RADIUS.

Configurar los tipos de autenticación global predeterminados

March 27, 2024

Al instalar NetScaler Gateway y ejecutar el asistente de NetScaler Gateway, configuró la autenticación en el asistente. Esta directiva de autenticación está vinculada automáticamente al nivel global de NetScaler Gateway. El tipo de autenticación que configura en el asistente de NetScaler Gateway es el tipo de autenticación predeterminado. Puede cambiar el tipo de autorización predeterminado ejecutando de nuevo el asistente de NetScaler Gateway o modificar la configuración de autenticación global en la utilidad de configuración.

Si necesita agregar tipos de autenticación adicionales, puede configurar directivas de autenticación en NetScaler Gateway y enlazar las directivas a NetScaler Gateway mediante la utilidad de configuración. Al configurar la autenticación de forma global, se define el tipo de autenticación, se configuran los valores y se establece el número máximo de usuarios que se pueden autenticar.

Después de configurar y vincular la directiva, puede establecer la prioridad para definir qué tipo de autenticación tiene prioridad. Por ejemplo, se configuran las directivas de autenticación LDAP y RADIUS. Si la directiva LDAP tiene un número de prioridad de 10 y la directiva RADIUS tiene un número de prioridad de 15, la directiva LDAP tiene prioridad, independientemente de dónde vincule cada directiva. Esto se denomina autenticación en cascada.

Puede elegir entregar páginas de inicio de sesión desde la memoria caché en memoria de NetScaler Gateway o desde el servidor HTTP que se ejecuta en NetScaler Gateway. Si decide entregar la página de inicio de sesión desde la memoria caché en memoria, la entrega de la página de inicio de sesión desde NetScaler Gateway es considerablemente más rápida que desde el servidor HTTP. La opción de entregar la página de inicio de sesión desde la memoria caché en memoria reduce el tiempo de espera cuando un gran número de usuarios inician sesión al mismo tiempo. Solo puede configurar la entrega de páginas de inicio de sesión desde la caché como parte de una directiva de autenticación global.

También puede configurar la dirección IP de traducción de direcciones de red (NAT) que es una dirección IP específica para la autenticación. Esta dirección IP es única para la autenticación y no es la subred de NetScaler Gateway, las direcciones IP asignadas ni las direcciones IP virtuales. Este es un parámetro opcional.

Nota: No se puede utilizar el asistente de NetScaler Gateway para configurar la autenticación SAML.

Puede utilizar el Asistente de configuración rápida para configurar la autenticación de certificados de cliente, LDAP y RADIUS. Al ejecutar el asistente, puede seleccionar entre un servidor LDAP o RADIUS existente configurado en NetScaler Gateway. También puede configurar los ajustes de LDAP o RADIUS. Si utiliza la autenticación de dos factores, Citrix recomienda utilizar LDAP como tipo de autenticación principal.

Para configurar la autenticación de forma global

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar la configuración de autenticación.
3. En Número máximo de usuarios, escriba el número de usuarios que se pueden autenticar mediante este tipo de autenticación.
4. En Dirección IP NAT, escriba la dirección IP única para la autenticación.
5. Seleccione Activar almacenamiento encaché estático para entregar las páginas de inicio de sesión más rápido.
6. Seleccione Habilitar comentarios de autenticación mejorada para enviar un mensaje a los usuarios si la autenticación falla. El mensaje que reciben los usuarios incluye errores de contraseña, cuenta inhabilitada o bloqueada, o no se encuentra al usuario, por nombrar algunos.
7. En Tipo de autenticación predeterminado, seleccione el tipo de autenticación.
8. Configure la configuración del tipo de autenticación y, a continuación, haga clic en Aceptar.

Configurar la autenticación sin autorización

January 26, 2024

La autorización define los recursos a los que los usuarios pueden conectarse a través de NetScaler Gateway. Las directivas de autorización se configuran mediante una expresión y, a continuación, se establece que se permita o deniegue la directiva. Puede configurar NetScaler Gateway para que utilice únicamente la autenticación, sin autorización.

Al configurar la autenticación sin autorización, NetScaler Gateway no realiza ninguna comprobación de autorización de grupo. Las directivas que configura para el usuario o el grupo se asignan al usuario.

Para obtener más información sobre cómo configurar la autorización, consulte Configuración de la autorización.

Configuración de autorización

January 26, 2024

La autorización especifica los recursos de red a los que tienen acceso los usuarios cuando inician sesión en NetScaler Gateway. La configuración predeterminada de la autorización es denegar el acceso a todos los recursos de red. Citrix recomienda utilizar la configuración global predeterminada y, a continuación, crear directivas de autorización para definir los recursos de red a los que pueden acceder los usuarios.

La autorización se configura en NetScaler Gateway mediante una directiva de autorización y expresiones. Después de crear una directiva de autorización, puede vincularla a los usuarios o grupos que haya configurado en el dispositivo.

Configuración de directivas de autorización

March 27, 2024

Al configurar una directiva de autorización, puede configurarla para permitir o denegar el acceso a los recursos de red de la red interna. Por ejemplo, para permitir que los usuarios accedan a la red 10.3.3.0, utilice la siguiente expresión:

CLIENT.IP.DST.IN_SUBNET (10.3.0.0/16)

Las directivas de autorización se aplican a usuarios y grupos. Después de autenticar a un usuario, NetScaler Gateway realiza una comprobación de autorización de grupo obteniendo la información del grupo del usuario de un servidor RADIUS, LDAP o TACACS+. Si la información del grupo está disponible para el usuario, NetScaler Gateway comprueba los recursos de red permitidos para el grupo.

Para controlar a qué recursos pueden acceder los usuarios, debe crear directivas de autorización. Si no necesita crear directivas de autorización, puede configurar la autorización global predeterminada.

Si crea una expresión dentro de la directiva de autorización que deniegue el acceso a una ruta de archivo, solo puede utilizar la ruta de acceso del subdirectorio y no el directorio raíz. Por ejemplo, use fs.path contiene ‘‘dir1dir2’’en lugar de fs.path contiene ‘‘rootdirdir1dir2’’. Si utiliza la segunda versión de este ejemplo, se produce un error en la directiva.

Después de configurar la directiva de autorización, la vinculará a un usuario o grupo como se muestra en las tareas siguientes.

De forma predeterminada, las directivas de autorización se validan primero con las directivas vinculadas al servidor virtual y, a continuación, con las directivas vinculadas globalmente. Si vincula una

directiva de forma global y quiere que la directiva global tenga prioridad sobre una directiva vinculada a un usuario, grupo o servidor virtual, puede cambiar el número de prioridad de la directiva. Los números de prioridad empiezan en cero. Un número de prioridad más bajo otorga a la directiva mayor prioridad.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el usuario tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

> **Importante:**
>
> - Las directivas de autorización clásicas solo se aplican al tráfico TCP.
> - La directiva de autorización avanzada se puede aplicar a todos los tipos de tráfico (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if “type”is not explicitly mentioned or “type”is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Para obtener más información sobre las directivas de autorización avanzadas, consulte el artículo https://support.citrix.com/article/CTX232237.

Ejemplos de expresiones de directiva de autorización

Estos son ejemplos de expresiones de directivas de autorización:

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")"ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.1 "DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv")|| CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)"ALLOW`

Para configurar una directiva de autorización mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Directivas > Autorización**.
2. En el panel de detalles, haga clic en **Agregar**.

3. En **Nombre**, escriba un nombre para la directiva.
4. En **Acción**, seleccione **Permitir** o **Denegar**.
5. En **Expresión** , haga clic en **Editor** de expresiones .
6. Para empezar a configurar la expresión, haga clic en **Seleccionar** y elija los elementos necesarios.
7. Haga clic en **Listo** cuando la expresión esté completa.
8. Haga clic en **Crear**.

Para enlazar una directiva de autorización a un usuario mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Administración de usuarios.**
2. Haga clic en **Usuarios AAA**.
3. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En **la página Vinculación** de directivas, seleccione una directiva o cree una directiva.
6. En **Prioridad**, defina el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

Para enlazar una directiva de autorización a un grupo mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway**> Administración de usuarios.
2. Haga clic en **Grupos AAA**.
3. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Modificar**.
4. En **Configuración avanzada**, haga clic en **Directivas de autorización**.
5. En **la página Vinculación** de directivas, seleccione una directiva o cree una directiva.
6. En **Prioridad**, defina el número de prioridad.
7. En **Tipo**, seleccione el tipo de solicitud y, a continuación, haga clic en **Aceptar**.

Configuración de la autorización global predeterminada

March 27, 2024

Para definir los recursos a los que tienen acceso los usuarios en la red interna, puede configurar la autorización global predeterminada. La autorización global se configura permitiendo o denegando el acceso a los recursos de red de forma global en la red interna.

Cualquier acción de autorización global que cree se aplica a todos los usuarios que aún no tengan una directiva de autorización asociada a ellos, ya sea directamente o a través de un grupo. Una directiva de autorización de usuarios o grupos siempre anula la acción de autorización global. Si la acción de autorización predeterminada se establece en Denegar, debe aplicar directivas de autorización para todos los usuarios o grupos para que esos usuarios o grupos puedan acceder a los recursos de red. Este requisito ayuda a mejorar la seguridad.

Para establecer la autorización global predeterminada:

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Seguridad, junto a Acción de autorización predeterminada, seleccione Permitir o Denegar y, a continuación, haga clic en Aceptar.

Inhabilitar la autenticación

March 27, 2024

Si la implementación no requiere autenticación, puede inhabilitarla. Puede inhabilitar la autenticación para cada servidor virtual que no requiera autenticación.

Importante: Citrix recomienda inhabilitar la autenticación con precaución. Si no utiliza un servidor de autenticación externo, cree usuarios y grupos locales para permitir que NetScaler Gateway autentique a los usuarios. Al inhabilitar la autenticación, se detiene el uso de funciones de autenticación, autorización y contabilidad que controlan y supervisan las conexiones a NetScaler Gateway. Cuando los usuarios escriban una dirección web para conectarse a NetScaler Gateway, la página de inicio de sesión no aparece.

Para inhabilitar la autenticación

1. En la utilidad de configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En la ficha Autenticación, en Autenticación de usuario, haga clic para desactivar Habilitar autenticación

Configurar la autenticación para horas específicas

March 27, 2024

Puede configurar una directiva de autenticación para que los usuarios tengan acceso a la red interna en momentos específicos, por ejemplo, durante el horario laboral normal. Cuando los usuarios intentan iniciar sesión en otro momento, se deniega el inicio de sesión.

Para restringir el momento en que los usuarios inician sesión en NetScaler Gateway, cree una expresión dentro de la directiva de autenticación y, a continuación, enlaza a un servidor virtual o de forma global.

Para configurar la autenticación por hora, fecha o día de la semana

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En Autenticación, seleccione el tipo de autenticación.
3. En el panel de detalles, haga clic en la ficha Directivas, seleccione una directiva de autenticación y, a continuación, haga clic en Abrir.
4. En el cuadro de diálogo Configurar directiva de autenticación, en Expresión, junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Fecha/hora.
6. En Qualifier, selecciona una de las siguientes opciones:

   - TIME para configurar el momento en que los usuarios no pueden iniciar sesión.
   - DATE para configurar la fecha en que los usuarios no pueden iniciar sesión.
   - DAYOFWEEK para configurar el día en que los usuarios no pueden iniciar sesión.

   Ejemplo: TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Lunes
7. En Operador, seleccione el valor.
8. En Valor, haga clic en el calendario junto al cuadro de texto y, a continuación, seleccione el día, la fecha u hora.
9. Haga clic en Aceptar dos veces, en Cerrar y haga clic en Aceptar.

Cómo funcionan las directivas de autenticación

January 26, 2024

Cuando los usuarios inician sesión en NetScaler Gateway, se autentican según una directiva creada por el usuario. La directiva define el tipo de autenticación. Una única directiva de autenticación se puede utilizar para necesidades de autenticación sencillas y suele estar vinculada a nivel global. También puede utilizar el tipo de autenticación predeterminado, que es local. Si configura la autenticación local, también debe configurar usuarios y grupos en NetScaler Gateway.

Puede configurar varias directivas de autenticación y vincularlas para crear un procedimiento de autenticación detallado y servidores virtuales. Por ejemplo, puede configurar la autenticación en cascada y en dos fases mediante la configuración de varias directivas. También puede establecer la prioridad de las directivas de autenticación para determinar qué servidores y el orden en que NetScaler Gateway comprueba las credenciales de usuario. Una directiva de autenticación incluye una expresión y una acción. Por ejemplo, si establece la expresión en True value, cuando los usuarios inician sesión, la acción evalúa el inicio de sesión del usuario como true y, a continuación, los usuarios tienen acceso a los recursos de red.

Después de crear una directiva de autenticación, la vincula a nivel global o a servidores virtuales. Al enlazar al menos una directiva de autenticación a un servidor virtual, las directivas de autenticación vinculadas al nivel global no se utilizan cuando los usuarios inician sesión en el servidor virtual, a menos que el tipo de autenticación global tenga una prioridad superior a la directiva vinculada al servidor virtual.

Cuando un usuario inicia sesión en NetScaler Gateway, la autenticación se evalúa en el siguiente orden:

- Se comprueba si hay directivas de autenticación vinculadas en el servidor virtual.
- Si las directivas de autenticación no están vinculadas al servidor virtual, NetScaler Gateway comprueba si hay directivas de autenticación globales.
- Si una directiva de autenticación no está vinculada a un servidor virtual ni de forma global, el usuario se autentica mediante el tipo de autenticación predeterminado.

Si configura directivas de autenticación LDAP y RADIUS y quiere enlazar las directivas de forma global para la autenticación de dos factores, puede seleccionar la directiva en la utilidad de configuración y, a continuación, seleccionar si la directiva es el tipo de autenticación principal o secundaria. También puede configurar una directiva de extracción de grupos.

Configurar perfiles de autenticación

March 27, 2024

Puede crear un perfil de autenticación mediante el asistente de NetScaler Gateway o la utilidad de configuración. El perfil contiene toda la configuración de la directiva de autenticación. El perfil se configura al crear la directiva de autenticación.

Con el asistente de NetScaler Gateway, puede utilizar el tipo de autenticación elegido para configurar la autenticación. Si quiere configurar directivas de autenticación adicionales después de ejecutar el asistente, puede utilizar la utilidad de configuración. Para obtener más información sobre el asistente de NetScaler Gateway, consulte Configuración de los ajustes mediante el Asistente de NetScaler Gateway.

Para crear una directiva de autenticación mediante la utilidad de configuración

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
4. Si utiliza un tipo de autenticación externa, junto a Servidor, haga clic en Nuevo.
5. En el cuadro de diálogo Crear servidor de autenticación, configure la configuración del tipo de autenticación, haga clic en Crear y, a continuación, haga clic en Cerrar.
6. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.
   Nota: Al seleccionar un tipo de autenticación y guardar el perfil de autenticación, no se puede cambiar el tipo de autenticación. Para utilizar un tipo de autenticación diferente, debe crear una nueva directiva.

Para modificar una directiva de autenticación mediante la utilidad de configuración

Puede modificar las directivas y los perfiles de autenticación configurados, como la dirección IP del servidor de autenticación o la expresión.

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Servidores, seleccione un servidor y, a continuación, haga clic en Abrir.

Para quitar una directiva de autenticación

Si ha cambiado o quitado un servidor de autenticación de la red, quite la directiva de autenticación correspondiente de NetScaler Gateway.

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En el panel de navegación, en Autenticación, seleccione un tipo de autenticación.
3. En el panel de detalles, en la ficha Directivas, seleccione una directiva y, a continuación, haga clic en Quitar.

Binding Authentication Policies

January 26, 2024

Después de configurar las directivas de autenticación, la vincula de forma global o a un servidor virtual. Puede utilizar la utilidad de configuración para enlazar una directiva de autenticación.

Para enlazar una directiva de autenticación de forma global mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.
2. Haga clic en un tipo de autenticación.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en un servidor y, a continuación, en **Acción**, haga clic en **Enlaces globales**.
4. En la ficha **Principal o Secundaria**, en **Detalles**, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

   Nota: Al seleccionar la directiva, NetScaler Gateway establece la expresión en True value automáticamente.

Para desenlazar una directiva de autenticación global mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.

2. En la pestaña **Políticas** , en **Acción** , haga clic en Enlaces **globales** .
3. **En el cuadro**de diálogo Vincular o desvincular las directivas de autenticación a las globales**, en la ficha**principal o secundaria**, en**Nombre de la directiva, seleccione la directiva**, haga clic en**Desvincular**la directiva y, a continuación, en Aceptar.**

Definir prioridades para directivas de autenticación

March 27, 2024

De forma predeterminada, las directivas de autenticación se validan primero con respecto a las directivas vinculadas al servidor virtual y, a continuación, con las directivas vinculadas globalmente. Si vincula una directiva de autenticación de forma global y quiere que la directiva global tenga prioridad sobre una directiva vinculada a un servidor virtual, puede cambiar el número de prioridad de la directiva. Los números de prioridad empiezan en cero. Un número de prioridad inferior otorga mayor prioridad a la directiva de autenticación.

Por ejemplo, si la directiva global tiene un número de prioridad de uno y el servidor virtual tiene una prioridad de dos, la directiva de autenticación global se aplica primero.

Para establecer o cambiar la prioridad de las directivas de autenticación global

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En la pestaña Políticas , en Acción , haga clic en Enlaces globales .
3. En el cuadro de diálogo Vincular o desvincular directivas globales de autenticación, en la ficha Principal o Secundaria, en Prioridad, escriba el número y, a continuación, haga clic en Aceptar.

Para cambiar la prioridad de una directiva de autenticación vinculada a un servidor virtual

También puede modificar una directiva de autenticación vinculada a un servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. Haga clic en la ficha Autenticación y seleccione Primaria o Secundaria.
4. Seleccione la directiva y, en Prioridad, escriba el número de la prioridad y, a continuación, haga clic en Aceptar.

Configurar usuarios locales

March 27, 2024

Puede crear cuentas de usuario localmente en NetScaler Gateway para complementar a los usuarios de los servidores de autenticación. Por ejemplo, puede que quiera crear cuentas de usuario locales para usuarios temporales, como consultores o visitantes, sin crear una entrada para esos usuarios en el servidor de autenticación.

Si utiliza la autenticación local, cree usuarios y, a continuación, agréguelos a los grupos que cree en NetScaler Gateway. Tras configurar usuarios y grupos, puede aplicar directivas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y los servidores a los que los usuarios tienen acceso.

Para crear usuarios locales

1. En la utilidad de configuración, haga clic en la pestaña **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de usuario**, escriba el nombre de usuario.
4. Si utiliza la autenticación local, desactive **Autenticación externa**.
   Nota: Seleccione **Autenticación externa** para que los usuarios se autentiquen en un servidor de autenticación externo, como LDAP o RADIUS. Desactive la casilla de verificación para que NetScaler Gateway se autentique en la base de datos de usuarios local.
5. En **Contraseña** y **Confirmar contraseña**, escriba la contraseña del usuario, haga clic en **Crear** y, a continuación, en **Cerrar**.

Para cambiar la contraseña de un usuario

Tras crear un usuario local, puede cambiar la contraseña del usuario o configurar la cuenta de usuario para que se autentique en un servidor de autenticación externo.

1. En la utilidad de configuración, haga clic en la pestaña **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Abrir**.
3. En **Contraseña** y **Confirmar contraseña**, escriba la nueva contraseña del usuario y, a continuación, haga clic en **Aceptar**.

Para cambiar el método de autenticación de un usuario

Si tiene usuarios configurados para la autenticación local, puede cambiar la autenticación por un servidor de autenticación externo. Para ello, habilite la autenticación externa.

1. En la utilidad de configuración, haga clic en la pestaña **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Abrir**.
3. Seleccione **Autenticación externa** y, a continuación, haga clic en **Aceptar**.

Para quitar un usuario

También puede quitar un usuario de NetScaler Gateway.

1. En la utilidad de configuración, haga clic en la pestaña **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un usuario y, a continuación, haga clic en **Quitar**.

Al quitar un usuario de NetScaler Gateway, todas las directivas asociadas también se quitan del perfil de usuario.

Configurar grupos

January 26, 2024

Puede tener grupos en NetScaler Gateway que sean grupos locales y que puedan autenticar a los usuarios con autenticación local. Si utiliza servidores externos para la autenticación, los grupos de NetScaler Gateway se configuran para que coincidan con los grupos configurados en los servidores de autenticación de la red interna. Cuando un usuario inicia sesión y se autentica, si el nombre de un grupo coincide con un grupo de un servidor de autenticación, el usuario hereda la configuración del grupo en NetScaler Gateway.

Una vez configurados los grupos, puede aplicar directivas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y los servidores a los que el usuario tiene acceso.

Si utiliza la autenticación local, cree usuarios y agréguelos a grupos configurados en NetScaler Gateway. A continuación, los usuarios heredan la configuración de ese grupo.

Importante: Si los usuarios son miembros de un grupo de Active Directory, el nombre del grupo de NetScaler Gateway debe ser el mismo que el del grupo de Active Directory.

Para crear un grupo

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo** , escriba un nombre para el grupo, haga clic en **Crear** y, a continuación, en **Cerrar** .

Para eliminar un grupo

También puede eliminar grupos de usuarios de NetScaler Gateway.

1. En la utilidad de configuración, haga clic en la ficha **Configuración** y, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, seleccione el grupo y, a continuación, haga clic en **Eliminar**.

Agregar usuarios a grupos

March 27, 2024

Puede agregar usuarios a un grupo durante la creación del grupo o posteriormente. Puede agregar usuarios a varios grupos para que los usuarios puedan heredar las directivas y la configuración vinculadas a esos grupos.

Para agregar usuarios a grupos:

1. **En la utilidad de configuración, haga clic en la ficha Configuración y, en el panel de navegación, expanda**NetScaler Gateway > Administración de usuarios**y, a continuación, haga clic en Usuarios AAA.**
2. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Abrir**.
3. En la ficha **Usuarios**, en **Usuarios disponibles, seleccione los usuarios**, haga clic en **Agregar** y, a continuación, en **Aceptar**.

Configurar directivas con grupos

January 26, 2024

Después de configurar los grupos, puede usar el cuadro de diálogo Grupo para aplicar directivas y configuraciones que especifiquen el acceso de los usuarios. Si utiliza la autenticación local, crea usuarios y los agrega a grupos configurados en NetScaler Gateway. A continuación, los usuarios heredan la configuración de ese grupo.

Puede configurar las siguientes directivas o ajustes para un grupo de usuarios en el cuadro de diálogo Grupo :

- Usuarios
- Directivas de autorización
- Directivas de auditoría
- Directivas de sesión
- Directivas de tráfico
- Marcadores
- Aplicaciones de intranet
- Direcciones IP de intranet

En la configuración, es posible que haya usuarios que pertenezcan a más de un grupo. Además, cada grupo puede tener una o más directivas de sesión vinculada, con parámetros diferentes configurados. Los usuarios que pertenecen a más de un grupo heredan las directivas de sesión asignadas a todos los grupos a los que pertenece el usuario. Para asegurarse de que la evaluación de directivas de sesión tiene prioridad sobre la otra, debe establecer la prioridad de la directiva de sesión.

Por ejemplo, tiene grupo1 enlazado con una directiva de sesión configurada con la página principal www.homepage1.com. Group2 está vinculado a una directiva de sesión configurada con la página principal www.homepage2.com. Cuando estas directivas están enlazadas a grupos respectivos sin un número de prioridad o con el mismo número de prioridad, la página principal que aparece a los usuarios que pertenecen a ambos grupos depende de la directiva que se procese primero. Al establecer un número de prioridad inferior, que otorga mayor prioridad, para la directiva de sesión con la página principal www.homepage1.com, puede asegurarse de que los usuarios que pertenecen a ambos grupos reciban la página principal www.homepage1.com.

Si las directivas de sesión no tienen asignado un número de prioridad o tienen el mismo número de prioridad, la prioridad se evalúa en el siguiente orden:

- Usuario
- Grupo
- Servidor virtual
- Global

Si las directivas están vinculadas al mismo nivel, sin número de prioridad o si las directivas tienen el mismo número de prioridad, el orden de evaluación es según el orden de vinculación de directivas. Las directivas vinculadas primero a un nivel tienen prioridad sobre las directivas vinculadas posteriormente.

Si tenemos un usuario vinculado a varios grupos con cada grupo enlazado a IIP, el usuario puede obtener IP libre de cualquiera de los grupos enlazados.

Configurar la autenticación LDAP

January 26, 2024

Puede configurar NetScaler Gateway para autenticar el acceso de los usuarios con uno o varios servidores LDAP.

La autorización LDAP requiere nombres de grupo idénticos en Active Directory, en el servidor LDAP y en NetScaler Gateway. Los caracteres y la caja también deben coincidir.

De forma predeterminada, la autenticación LDAP es segura mediante la Secure Sockets Layer (SSL) o la Transport Layer Security (TLS). Existen dos tipos de conexiones LDAP seguras. Con un tipo, el servidor LDAP acepta las conexiones SSL o TLS en un puerto independiente del puerto que utiliza el servidor LDAP para aceptar conexiones LDAP claras. Una vez que los usuarios establecen las conexiones SSL o TLS, el tráfico LDAP se puede enviar a través de la conexión.

Los números de puerto de las conexiones LDAP son:

- 389 para conexiones LDAP no seguras
- 636 para conexiones LDAP seguras
- 3268 para conexiones LDAP no seguras de Microsoft
- 3269 para conexiones LDAP seguras de Microsoft

El segundo tipo de conexiones LDAP seguras utiliza el comando StartTLS y utiliza el número de puerto 389. Si configura los números de puerto 389 o 3268 en NetScaler Gateway, el servidor intenta usar StartTLS para establecer la conexión. Si utiliza cualquier otro número de puerto, el servidor intenta establecer conexiones mediante SSL o TLS. Si el servidor no puede utilizar StartTLS, SSL o TLS, la conexión falla.

Si especifica el directorio raíz del servidor LDAP, NetScaler Gateway busca en todos los subdirectorios el atributo de usuario. En directorios grandes, este enfoque puede afectar al rendimiento. Por este motivo, Citrix recomienda utilizar una unidad organizativa (OU) específica.

La tabla siguiente contiene ejemplos de campos de atributos de usuario para servidores LDAP:

Servidor LDAP	atributo de usuario	Sensible a may
Servidor Microsoft Active Directory	sAMAccountName	No
Directorio electrónico de Novell	ou	Sí
Servidor IBM Directory	uid	Sí
Lotus Domino	CN	Sí
Directorio Sun ONE (anteriormente iPlanet)	uid o cn	Sí

Esta tabla contiene ejemplos del DN base:

Servidor LDAP	DN base
Servidor Microsoft Active Directory	DC=citrix, DC = local
Directorio electrónico de Novell	ou=users, ou=dev
Servidor IBM Directory	cn=usuarios
Lotus Domino	OU=Ciudad, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	ou=Personas, dc=citrix, dc=com

La tabla siguiente contiene ejemplos de DN de enlace:

Servidor LDAP	Vincular DN
Servidor Microsoft Active Directory	CN=Administrador, CN=Usuarios, DC=citrix, DC=local
Directorio electrónico de Novell	cn=admin, o=citrix
Servidor IBM Directory	LDAP_dn
Lotus Domino	CN=Administrador de notas, O=Citrix, C=US
Directorio Sun ONE (anteriormente iPlanet)	uid=admin, ou=Administradores, ou=topologyManagement, o=netscaperoot

Nota: Para obtener más información sobre la configuración del servidor LDAP, consulte Determinación de atributos en el directorio LDAP.

Para configurar la autenticación LDAP mediante la utilidad de configuración

January 26, 2024

1. Vaya a **NetScaler Gateway** >**Directivas** > **Autenticación**.
2. Haga clic en **LDAP**.
3. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
4. En **Nombre**, escriba un nombre para la directiva.
5. Junto a **Servidor** , haz clic en **Nuevo** .
6. En **Nombre**, escriba el nombre del servidor.
7. En **Servidor**, en **Dirección IP y puerto**, escriba la dirección IP y el número de puerto del servidor LDAP.
8. En **Tipo**, seleccione **AD** para Active Directory o **NDS** para Novell Directory Services.
9. En **Configuración de conexión**, complete lo siguiente:

   a) En **DN base (ubicación de los usuarios)**, escriba el DN base en el que se encuentran los usuarios. DN base busca los usuarios ubicados en el directorio seleccionado (AD o NDS).

   El DN base se deriva del DN de enlace eliminando el nombre de usuario y especificando el grupo en el que se encuentran los usuarios. Ejemplos de la sintaxis del DN base son:

   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   b) En **Administrator Vincular DN**, escriba el DN de enlace de administrador para las consultas al directorio LDAP. Algunos ejemplos de la sintaxis de bind DN son:

   ```
   domain/user name
   ou=administrator,dc=ace,dc=com
   user@domain.name (for Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   Para Active Directory, se requiere el nombre del grupo especificado como cn=groupname. El nombre del grupo definido en NetScaler Gateway y el nombre del grupo en el servidor LDAP deben ser idénticos.

   Para otros directorios LDAP, el nombre del grupo no es obligatorio o, si es necesario, se especifica como ou=groupname.

NetScaler Gateway se vincula al servidor LDAP mediante las credenciales de administrador y, a continuación, busca al usuario. Tras localizar al usuario, NetScaler Gateway desvincula las credenciales de administrador y vuelve a enlazar con las credenciales de usuario.

c) En **Contraseña de administrador y Confirmar contraseña**de administrador, escriba la contraseña de administrador del servidor LDAP.

10. Para recuperar automáticamente más ajustes de LDAP, haga clic en **Recuperar atributos**.

    Al hacer clic en **Recuperar atributos**, los campos de Otros ajustes se rellenan automáticamente. Si quiere ignorar este paso, continúe con los pasos 12 y 13. De lo contrario, vaya al paso 14.

11. En **Otras opciones**, en Atributo de nombre de inicio de sesión del servidor, escriba el atributo con el que NetScaler Gateway debe buscar los nombres de inicio de sesión de usuario del servidor LDAP que va a configurar. El valor predeterminado es `samAccountName`.

12. En **Filtro de búsqueda**, escriba el valor para buscar los usuarios asociados a uno o varios grupos de active directory.

    Por ejemplo, "memberOf=CN=GatewayAccess, OU=Groups, DC=Users, DC=lab".

    > **Nota**
    >
    > Puede utilizar el ejemplo anterior para restringir el acceso de NetScaler Gateway solo a los miembros de un grupo de AD específico.

13. En **Atributo de grupo**, deje el memberOf predeterminado para Active Directory o cambie el atributo por el atributo del tipo de servidor LDAP que está usando. Este atributo permite a NetScaler Gateway obtener los grupos asociados a un usuario durante la autorización.

14. En Tipo **de seguridad**, seleccione el tipo de seguridad y, a continuación, haga clic en **Crear**.

15. Para permitir a los usuarios cambiar su contraseña LDAP, seleccione **Permitir cambio de contraseña**.

    Nota:

    - Si selecciona **TEXTO SIN FORMATO** como tipo de seguridad, no se admite la posibilidad de que los usuarios cambien sus contraseñas.
    - Si selecciona **PLAINTTEXT** o **TLS por motivos** de seguridad, utilice el número de puerto 389. Si selecciona **SSL**, utilice el número de puerto 636.

Determine los atributos de su directorio LDAP

March 27, 2024

Si necesita ayuda para determinar los atributos de su directorio LDAP para poder configurar los ajustes de autenticación en NetScaler Gateway, puede buscarlos fácilmente con el explorador LDAP gratuito de Softerra.

Puede descargar el explorador LDAP desde el sitio web de Softerra LDAP Administrator. Después de instalar el explorador, defina los siguientes atributos:

- El nombre de host o la dirección IP del servidor LDAP.
- El puerto del servidor LDAP. El valor por defecto es 389.
- El campo DN base, que puede dejar en blanco. La información proporcionada por el explorador LDAP puede ayudarle a determinar el DN base que debe configurar esta opción en NetScaler Gateway.
- La comprobación Enlace anónimo determina si el servidor LDAP requiere credenciales de usuario para conectarse a él. Si el servidor LDAP requiere credenciales, deje la casilla de verificación desactivada.

Después de completar la configuración, el explorador LDAP muestra el nombre del perfil en el panel izquierdo y se conecta al servidor LDAP.

Configurar la extracción de grupos LDAP

January 26, 2024

Si utiliza la autenticación de dos factores, los grupos extraídos de las fuentes de autenticación principal y secundaria se concatenan. Las directivas de autorización se pueden aplicar al grupo que se extrae del servidor de autenticación principal o secundario.

Los nombres de grupo obtenidos del servidor LDAP se comparan con los nombres de grupo creados localmente en NetScaler Gateway. Si los nombres de los dos grupos coinciden, las propiedades del grupo local se aplican al grupo obtenido de los servidores LDAP.

Si los usuarios pertenecen a más de un grupo LDAP, NetScaler Gateway extrae información de usuarios de todos los grupos a los que pertenecen los usuarios. Si un usuario es miembro de dos grupos en NetScaler Gateway y cada grupo tiene una directiva de sesión vinculada, el usuario hereda las directivas de sesión de ambos grupos. Para asegurarse de que los usuarios reciben la directiva de sesión correcta, establezca la prioridad de la directiva de sesión.

Para obtener más información sobre los atributos de pertenencia a grupos LDAP, consulte lo siguiente:

- Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario
- Cómo funciona indirectamente la extracción de grupos LDAP desde el objeto de grupo

Cómo funciona la extracción de grupos LDAP directamente desde el objeto de usuario

January 26, 2024

Los servidores LDAP que evalúan la pertenencia a grupos desde objetos de grupo admiten la autorización de NetScaler Gateway.

Algunos servidores LDAP permiten que los objetos de usuario contengan información sobre los grupos a los que pertenecen los objetos, como Active Directory (mediante el atributo memberOf) o IBM eDirectory (mediante el atributo groupMembership). La pertenencia al grupo de un usuario puede ser atributos del objeto de usuario, como IBM Directory Server (mediante IBM-AllGroups) o el servidor de directorios Sun ONE (mediante NSRole). Ambos tipos de servidores LDAP admiten la extracción de grupos de NetScaler Gateway.

Por ejemplo, en IBM Directory Server, todas las pertenencias a grupos, incluidos los grupos estáticos, dinámicos y anidados, se pueden devolver mediante el atributo IBM-AllGroups. En Sun ONE, todas las funciones, incluidas las administradas, filtradas y anidadas, se calculan mediante el atributo NSRole.

Cómo funciona indirectamente la extracción de grupos LDAP desde el objeto de grupo

January 26, 2024

Los servidores LDAP que evalúan la pertenencia a grupos desde objetos de grupo de forma indirecta no son compatibles con la autorización de NetScaler Gateway.

Algunos servidores LDAP, como Lotus Domino, permiten que los objetos de grupo solo contengan información sobre los usuarios. Estos servidores LDAP no permiten que el objeto de usuario contenga información sobre grupos y, por lo tanto, no son compatibles con la extracción de grupos de NetScaler Gateway. Para este tipo de servidor LDAP, las búsquedas de pertenencia a grupos se realizan ubicando al usuario en la lista de miembros de grupos.

Campos de atributo de grupo de autorización LDAP

January 26, 2024

En la tabla siguiente se incluyen ejemplos de campos de atributos de grupo LDAP:

Servidores LDAP	atributo LDAP
Servidor Microsoft Active Directory	Miembro de
Directorio electrónico de Novell	Pertenencia a
Servidor IBM Directory	IBM - Todos los grupos
Directorio Sun ONE (anteriormente iPlanet)	NSrol

Para configurar la autorización LDAP

March 27, 2024

Para configurar la autorización LDAP en la directiva de autenticación, defina el nombre del atributo de grupo y el subatributo.

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En Autenticación, haga clic en un tipo de autenticación.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. Junto a Servidor , haz clic en Nuevo .
6. En Nombre, escriba el nombre del servidor.
7. En Servidor, escriba la dirección IP y el puerto del servidor LDAP.
8. En Atributo de grupo, escriba memberOf.
9. En Nombre de subatributo, escriba CN y, a continuación, haga clic en Crear.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

Configurar la extracción de grupos anidados LDAP

March 27, 2024

NetScaler Gateway puede consultar grupos LDAP y extraer información de grupos y usuarios de grupos antiguos configurados en el servidor de autenticación. Por ejemplo, creaste grupo1 y dentro de

ese grupo creaste grupo2 y grupo3. Si el usuario pertenece al grupo3, NetScaler Gateway extrae información de todos los grupos antiguos anidados (grupo2, grupo1) hasta el nivel especificado.

Puede utilizar una directiva de autenticación para configurar la extracción de grupos anidados de LDAP. Cuando se ejecuta la consulta, NetScaler Gateway busca en los grupos hasta que alcanza el nivel máximo de anidamiento o hasta que busca en todos los grupos disponibles.

Para configurar la extracción de grupos anidados de LDAP

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Autenticación/autorización > Autenticación > Autenticación** y, a continuación, haga clic en **LDAP**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Servidor, haga clic en **Nuevo**.
5. En Nombre, escriba el nombre del servidor.
6. Configure los ajustes del servidor LDAP.
7. Expanda **Extracción de grupos anidados**y haga clic en **Habilitar**.
8. En **Nivel máximo de anidamiento**, escriba el número de niveles que comprueba NetScaler Gateway.
9. En **Identificador de nombre de grupo**, escriba el nombre del atributo LDAP que identifica de forma exclusiva un nombre de grupo en el servidor LDAP, como `sAMAccountName`.
10. En **Atributo de búsqueda de grupo**, escriba el nombre del atributo LDAP que se va a obtener en la respuesta de búsqueda para determinar los grupos principales de cualquier grupo. Por ejemplo: `memberOf`.
11. En **Subatributo de búsqueda de grupos**, escriba el nombre del subatributo LDAP que se va a buscar como parte del atributo de búsqueda de grupos para determinar los grupos principales de cualquier grupo. Por ejemplo, escriba CN.
12. En **Filtro de búsqueda de grupo**, escriba la cadena de consulta. Por ejemplo, el filtro puede ser `&(samaccountname=test)(objectClass=\*)`.
13. Haga clic en **Crear**y, a continuación, en **Cerrar**.
14. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Configurar la extracción de grupos LDAP para varios dominios

January 26, 2024

Si tiene varios dominios para la autenticación y utiliza StoreFront o la Interfaz Web, puede configurar NetScaler Gateway para que utilice la extracción de grupos para enviar el nombre de dominio correcto a la interfaz web.

En Active Directory, debe crear un grupo para cada dominio de la red. Después de crear el grupo, agrega usuarios que pertenecen al grupo y al dominio especificado. Una vez configurados los grupos en Active Directory, debe configurar la extracción de grupos LDAP para varios dominios en NetScaler Gateway.

Para configurar NetScaler Gateway para la extracción de grupos de varios dominios, debe crear el mismo número de directivas de sesión y autenticación que el número de dominios de la red. Por ejemplo, tiene dos dominios, denominados Sampa y Child. Cada dominio recibe una directiva de sesión y una directiva de autenticación.

Después de crear las directivas, crea grupos en NetScaler Gateway y vincula las directivas de sesión al grupo. A continuación, vincula las directivas de autenticación a un servidor virtual.

Si implementa StoreFront en varios dominios, debe haber una relación de confianza entre los dominios.

Si implementa Citrix Endpoint Management o la interfaz web en varios dominios, no es necesario que los dominios confíen entre sí.

Crear directivas de sesión para la extracción de grupos

March 27, 2024

El primer paso al crear directivas de sesión para la extracción de grupos consiste en crear dos perfiles de sesión y establecer los siguientes parámetros:

- Habilite el proxy ICA.
- Agregue la dirección web de la interfaz Web.
- Agregue el dominio de Windows.
- Agregue el perfil a una directiva de sesión y defina la expresión en true.

Para crear los perfiles de sesión para la extracción grupal

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway > Directivas**y, a continuación, haga clic en Sesión.**
2. En el panel de detalles, haga clic en la pestaña **Perfiles** y, a continuación, en **Agregar** .
3. En **Nombre**, escriba un nombre para el perfil. Por ejemplo, escriba Sampa.
4. En la ficha **Aplicaciones publicadas**, haga lo siguiente:

a) Junto a **ICA Proxy**, haga clic en **Supeditación global** y, a continuación, seleccione **ACTIVADO**.
b) Junto a **Dirección de interfaz web**, haga clic en **Supeditación global** y, a continuación, escriba la dirección web de la interfaz web.
c) Junto a **Dominio de inicio de sesión único, haga clic enSobrescribir global**, escribe el nombre del dominio de Windows y, a continuación, haga clic en**Crear**.

5. En **Nombre**, borre el nombre del primer dominio y escriba el nombre del segundo dominio, por ejemplo, Hijo.
6. Junto a **Dominio de inicio de sesión único**, borre el nombre del primer dominio de Windows y escriba el nombre del segundo dominio, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear los perfiles de sesión, crea dos directivas de sesión. Cada directiva de sesión utiliza uno de los perfiles.

Para crear una directiva de sesión

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway > Directivas**y, a continuación, haga clic en Sesión.**
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Solicitar perfil**, seleccione el perfil del primer dominio.
5. Junto a **Expresiones con nombre**, haga clic en **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión y,** a continuación, haga clic en **Crear**.
6. En **Nombre**, cambie el nombre al segundo dominio.
7. En **Solicitar perfil**, seleccione el perfil del segundo dominio, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Crear directivas de autenticación LDAP para varios dominios

March 27, 2024

Después de crear directivas de sesión en NetScaler Gateway, crea directivas de autenticación LDAP casi idénticas. Al configurar la directiva de autenticación, el campo importante es Filtro de búsqueda. En este campo, debe escribir el nombre del grupo que creó en Active Directory.

Cree primero los perfiles de autenticación y, a continuación, cree la directiva de autenticación.

Para crear perfiles de autenticación para varias extracciones de grupos de dominios

1. En la utilidad de configuración, en la ficha Configuración, expanda Citrix **Gateway > Directivas > Autenticación**.
2. En el panel de navegación, haga clic en **LDAP**.
3. En el panel de detalles, haga clic en la ficha **Servidores** y, a continuación, en **Agregar**.
4. En **Nombre**, escriba el nombre del primer dominio, como `Sampa`.
5. Configure la configuración del servidor LDAP y, a continuación, haga clic en **Crear**.
6. Repita los pasos 3, 4 y 5 para configurar el perfil de autenticación del segundo dominio y, a continuación, haga clic en **Cerrar**.

Después de crear y guardar los perfiles, cree las directivas de autenticación.

Para crear directivas de autenticación para varias extracciones de grupos de dominios

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.
2. En el panel de detalles, haga clic en la ficha **Directivas** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, escriba el nombre del primer dominio.
4. En **Tipo de autenticación**, seleccione **LDAP**.
5. En **Servidor**, seleccione el perfil de autenticación del primer dominio.
6. Junto a **Expresiones con nombre**, haga clic en **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión y,** a continuación, haga clic en **Crear**.
7. En Nombre, escriba el nombre del segundo dominio.
8. En **Servidor**, seleccione el perfil de autenticación del segundo dominio, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Crear grupos y directivas de enlace para la extracción de grupos LDAP para varios dominios

March 27, 2024

Después de crear directivas de autenticación, crea grupos en NetScaler Gateway. Después de crear los grupos, vincula la directiva de autenticación a un servidor virtual.

Para crear grupos en NetScaler Gateway

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios** y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo**, escriba el nombre del primer grupo de Active Directory.
   Importante: Al crear grupos en NetScaler Gateway para la extracción de grupos de varios dominios, los nombres de los grupos deben ser los mismos que los grupos definidos en Active Directory. Los nombres de grupo también distinguen entre mayúsculas y minúsculas y las mayúsculas deben coincidir con las mayúsculas y min
4. En la ficha **Directivas**, haga clic en **Sesión** y, a continuación, en **Insertar directiva**.
5. En **Nombre de la directiva**, haga doble clic en la directiva y, a continuación, haga clic en **Crear**.

Para enlazar las directivas de autenticación a un servidor virtual

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha Autenticación, haga clic en **Principal**, en **Nombre de la directiva**, haga doble clic en **Insertar directiva** y, a continuación, seleccione la primera directiva de autenticación.
4. En **Nombre de la directiva**, haga clic en **Insertar directiva**, haga doble clic en la segunda directiva de autenticación y, a continuación, haga clic en **Aceptar**.

Notificación de caducidad de contraseñas de 14 días para la autenticación LDAP

January 26, 2024

El dispositivo NetScaler Gateway admite la notificación de caducidad de contraseñas de 14 días para la autenticación basada en LDAP. Al usar esta función, los administradores pueden notificar a los usuarios finales sobre el tiempo límite de caducidad de la contraseña en días. Para obtener más información, consulte Notificación de caducidad de contraseñas de 14 días para la autenticación LDAP.

Configuración de la autenticación con certificados del cliente

January 26, 2024

Los usuarios que inician sesión en un servidor virtual de NetScaler Gateway también se pueden autenticar en función de los atributos de certificado de cliente presentados en el servidor virtual. La autenticación de certificados de cliente también se puede utilizar con otros tipos de autenticación, como LDAP o RADIUS, para proporcionar autenticación de dos factores.

Para autenticar a los usuarios en función de los atributos del certificado del lado del cliente, la autenticación del cliente debe estar habilitada en el servidor virtual y se debe solicitar el certificado de cliente. Es necesario vincular un certificado raíz al servidor virtual en NetScaler Gateway.

Cuando los usuarios inician sesión en el servidor virtual de NetScaler Gateway, tras la autenticación, la información del nombre de usuario se extrae del campo especificado del certificado. Normalmente, este campo es Sujeto:CN. Si el nombre de usuario se extrae correctamente, se puede autenticar al usuario con éxito. La autenticación falla en los siguientes casos.

- Si el usuario no proporciona un certificado válido durante el enlace de Secure Sockets Layer (SSL).
- La extracción del nombre de usuario falla, la autenticación falla.

Se puede autenticar usuarios basándose en el certificado del cliente, definiendo el tipo de autenticación predeterminado para que use el certificado del cliente. También se puede crear una acción de certificado que defina lo que hay que hacer durante la autenticación basada en un certificado SSL del cliente.

Para configurar el certificado de cliente como el tipo de autenticación predeterminado mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway y,** a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración de autenticación**, haga clic en **Cambiar la configuración de CERT de autenticación**.
3. Seleccione **ACTIVADO** para habilitar la autenticación de dos factores mediante el certificado según sus necesidades.
4. En **Campo Nombre de usuario**, seleccione el tipo de campo de certificado que contiene los nombres de usuario.
5. En **Campo Nombre de Grupo**, seleccione el tipo de campo de certificado que contiene el nombre del grupo.
6. En **Grupo de autorización predeterminado**, escriba el nombre del grupo predeterminado y, a continuación, haga clic en **Aceptar**.

Extracción del nombre de usuario del certificado de cliente

Si la autenticación de certificados del cliente está habilitada en NetScaler Gateway, los usuarios se autenticarán basándose en ciertos atributos del certificado del cliente. Una vez que la autenticación se realiza correctamente, el nombre de usuario o el nombre de usuario y grupo del usuario se extraen del certificado. Además, se aplican las directivas especificadas para ese usuario.

Configuring and Binding a Client Certificate Authentication Policy

March 27, 2024

Puede crear una directiva de autenticación de certificados de cliente y vincularla a un servidor virtual. Puede utilizar la directiva para restringir el acceso a grupos o usuarios específicos. Esta directiva tiene prioridad sobre la directiva global.

Para configurar una directiva de autenticación de certificados de cliente:

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.
2. En el panel de navegación, en **Autenticación**, haga clic en **CERT**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En **el campo Nombre**, escriba un nombre para la directiva.
5. Junto a **Servidor** , haz clic en **Nuevo** .
6. En **Nombre**, escriba un nombre para el perfil.
7. Junto a **Dos factores**, selecciona **DESACTIVADO**.
8. En los campos **Nombre de usuario** y **Nombre de grupo**, seleccione los valores y, a continuación, haga clic en &**Crear**.
   Nota: Si configuró previamente los certificados de cliente como el tipo de autenticación predeterminado, utilice los mismos nombres que utilizó para la directiva. Si ha completado los campos Nombre de
   usuario y Nombre de
   grupo para el tipo de autenticación predeterminado, utilice los mismos valores para el perfil.
9. En el cuadro de diálogo **Crear directiva de autenticación**, junto a **Expresiones con nombre**, seleccione la expresión, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Para enlazar una directiva de certificados de cliente a un servidor virtual:

Después de configurar la directiva de autenticación de certificados de cliente, puede vincularla a un servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.

2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en **Abrir** .
3. En el cuadro de diálogo **Configurar el servidor virtual NetScaler Gateway**, haga clic en la ficha **Autenticación**.
4. Haga clic en **Primaria** o **Secundaria**
5. En **Detalles**, haga clic en **Insertar directiva**.
6. En **Nombre de la política** , seleccione la política y, a continuación, haga clic **en**Aceptar .

Para configurar un servidor virtual de modo que solicite el certificado de cliente:

Si quiere utilizar un certificado de cliente para la autenticación, debe configurar el servidor virtual para que se soliciten certificados de cliente durante el enlace SSL.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un **servidor virtual** y, a continuación, haga clic en **Abrir**.
3. En la ficha **Certificados**, haga clic en **Parámetro SSL**.
4. En **Otros**, haga clic en **Autenticación de cliente**
5. En **Certificado de cliente**, seleccione **Opcional** u **Obligatorio** y haga clic en Aceptar dos veces. Seleccione **Opcional** si quiere permitir otros tipos de autenticación en el mismo servidor virtual y no requiere el uso de certificados de cliente.

> **Nota**
>
> - Para obtener más información sobre la URL de devolución de llamada, consulte Importar un NetScaler Gateway.
> - Para obtener más información sobre los certificados, consulte Instalar, vincular y actualizar certificados.

Configurar la autenticación de certificados de cliente de dos factores

January 26, 2024

Puede configurar un certificado de cliente para autenticar primero a los usuarios y, a continuación, solicitar a los usuarios que inicien sesión con un tipo de autenticación secundario, como LDAP o RADIUS. En este caso, el certificado de cliente autentica primero a los usuarios. A continuación, aparece una página de inicio de sesión en la que pueden introducir su nombre de usuario y contraseña. Cuando se completa el enlace de Secure Sockets Layer (SSL), la secuencia de inicio de sesión puede tomar una de las dos rutas siguientes:

- Ni el nombre de usuario ni el grupo se extraen del certificado. La página de inicio de sesión aparece al usuario con un mensaje para que introduzca credenciales de inicio de sesión válidas.

NetScaler Gateway autentica las credenciales de usuario como en el caso de la autenticación de contraseña normal.

- El nombre de usuario y el nombre del grupo se extraen del certificado de cliente. Si solo se extrae el nombre de usuario, aparece una página de inicio de sesión para el usuario en el que está presente el nombre de inicio de sesión y el usuario no puede modificar el nombre. Solo el campo de contraseña está en blanco.

La información de grupo que NetScaler Gateway extrae durante la segunda ronda de autenticación se anexa a la información del grupo, si la hay, que NetScaler Gateway extrajo del certificado.

Configurar la autenticación con tarjeta inteligente

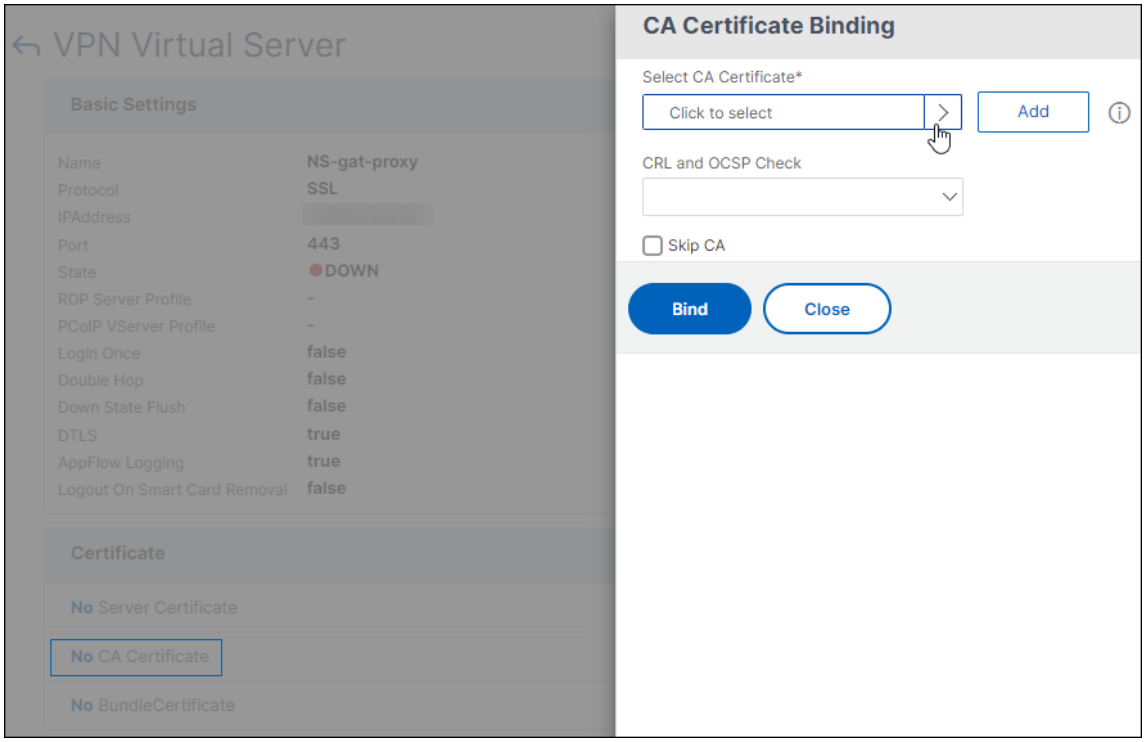
March 27, 2024

Puede configurar NetScaler Gateway para que utilice una tarjeta inteligente criptográfica para autenticar a los usuarios.

Para configurar una tarjeta inteligente con NetScaler Gateway, debe hacer lo siguiente:

- Cree una directiva de autenticación de certificados. Para obtener más información, consulte Configuración de la autenticación de certificados de cliente.
- Enlazar la directiva de autenticación a un servidor virtual.
- Agregue el certificado raíz de la entidad emisora de certificados (CA) que emite los certificados de cliente a NetScaler Gateway. Para obtener más información, consulte Para instalar un certificado raíz en NetScaler Gateway.

  Importante: Al agregar el certificado raíz al servidor virtual para la autenticación con tarjeta inteligente, debe seleccionar el certificado en la lista
  Seleccionar certificado de CA.



Después de crear el certificado de cliente, puede escribir el certificado, conocido como flash, en la tarjeta inteligente. Cuando complete este paso, podrá probar la tarjeta inteligente.

Si configura la interfaz web para la autenticación de acceso directo con tarjeta inteligente, si se da alguna de las siguientes condiciones, se produce un error en el inicio de sesión único en la interfaz web:

- Si establece el dominio en la ficha **Aplicaciones publicadas** como `mydomain`.com en lugar de `mydomain`.
- Si no establece el nombre de dominio en la ficha **Aplicaciones publicadas** y si ejecuta el comando `wi-sso-split-upn` al establecer el valor en 1. En este caso, UserPrincipalName contiene el nombre de dominio "`mydomain`.com".

Puede utilizar la autenticación con tarjeta inteligente para optimizar el proceso de inicio de sesión de 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 factores basada en certificados mediante la 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 inicien sesión en StoreFront también pueden acceder a las aplicaciones pro-

porcionadas por NetScaler Endpoint Management. Sin embargo, los usuarios deben autenticarse de nuevo para acceder a las aplicaciones web de Endpoint Management que utilizan la autenticación de certificados de cliente.

Para obtener más información, consulte Configurar la autenticación con tarjeta inteligente en la documentación de StoreFront.

Configuración de la autenticación de tarjeta inteligente con conexiones ICA seguras

Los usuarios que inician sesión y establecen una conexión ICA segura mediante una tarjeta inteligente con inicio de sesión único configurado en NetScaler Gateway pueden recibir dos solicitudes de su número de identificación personal (PIN).

- Al iniciar sesión y al intentar iniciar un recurso publicado. Esta situación se produce si el explorador web y la aplicación Citrix Workspace utilizan el mismo servidor virtual que está configurado para usar certificados de cliente.
- La aplicación Citrix Workspace no comparte ningún proceso ni una conexión de Secure Sockets Layer (SSL) con el explorador web. Por lo tanto, cuando la conexión ICA completa el protocolo de enlace SSL con NetScaler Gateway, se requiere el certificado de cliente por segunda vez.

Para evitar que los usuarios reciban la segunda solicitud de PIN, tiene que cambiar dos configuraciones:

- La autenticación de cliente en el servidor virtual de VPN debe estar inhabilitada.
- La renegociación SSL debe estar habilitada.

Después de configurar el servidor virtual, vincule uno o varios servidores STA al servidor virtual, como se describe en Configuración de los parámetros de NetScaler Gateway en la Interfaz Web 5.3.

Es posible que también quieras probar la autenticación con tarjeta inteligente.

Para inhabilitar la autenticación de cliente:

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. Seleccione el servidor virtual correspondiente en el panel de detalles principal y, a continuación, haga clic en Modificar.
3. En el panel Opciones avanzadas, haga clic en Parámetros SSL.
4. Desactive la casilla Autenticación de cliente.
5. Haga clic en Listo.

Para habilitar la renegociación SSL:

1. Con la utilidad de configuración, en la ficha Configuración, vaya a Administración del tráfico y, a continuación, haga clic en SSL.

2. En el panel principal, haga clic en Cambiar la configuración avanzada de SSL.
3. En el menú Denegar renegociación de SSL, seleccione NO.

Para probar la autenticación con tarjeta inteligente:

1. Conecte la tarjeta inteligente al dispositivo del usuario.
2. Abra el explorador web e inicie sesión en NetScaler Gateway.

Configurar la autenticación RADIUS

January 26, 2024

Puede configurar NetScaler Gateway para autenticar el acceso de los usuarios con uno o varios servidores RADIUS. Si utiliza productos RSA SecurID, SafeWord o Gemalto Protiva, cada uno de estos productos se configura mediante un servidor RADIUS.

Es posible que su configuración requiera el uso de una dirección IP del servidor de acceso a la red (IP del NAS) o un identificador del servidor de acceso a la red (ID del NAS). Al configurar NetScaler Gateway para utilizar un servidor de autenticación RADIUS, siga las siguientes pautas:

- Si habilita el uso de la IP del NAS, el dispositivo envía su dirección IP configurada al servidor RADIUS, en lugar de la dirección IP de origen utilizada para establecer la conexión RADIUS.
- Si configura el ID del NAS, el dispositivo envía el identificador al servidor RADIUS. Si no configura el ID del NAS, el dispositivo envía su nombre de host al servidor RADIUS.
- Al habilitar la IP del NAS, el dispositivo ignora cualquier ID del NAS configurado mediante la IP del NAS para comunicarse con el servidor RADIUS.

Configuración de Gemalto Protiva

Protiva es una sólida plataforma de autenticación desarrollada por Gemalto para utilizar los puntos fuertes de la autenticación con tarjeta inteligente de Gemalto. Con Protiva, los usuarios inician sesión con un nombre de usuario, una contraseña y una contraseña de un solo uso que genera el dispositivo Protiva. Al igual que RSA SecurID, la solicitud de autenticación se envía al servidor de autenticación de Protiva y el servidor valida o rechaza la contraseña. Para configurar Gemalto Protiva para que sea compatible con NetScaler Gateway, siga las siguientes pautas:

- Instale el servidor Protiva.
- Instale el software Protiva SAS Agent, que amplía el servidor de autenticación de Internet (IAS), en un servidor RADIUS de Microsoft IAS. Asegúrese de anotar la dirección IP y el número de puerto del servidor IAS.

- Configure un perfil de autenticación RADIUS en NetScaler Gateway e introduzca la configuración del servidor Protiva.

Configuración de SafeWord

La línea de productos SafeWord proporciona autenticación segura mediante un código de acceso basado en tokens. Una vez que el usuario introduce el código, SafeWord invalida inmediatamente el código de acceso y no se puede volver a utilizar. Al configurar el servidor SafeWord, necesita la siguiente información:

- Dirección IP de NetScaler Gateway. La dirección IP debe ser la misma dirección IP que configuró en la configuración del cliente del servidor RADIUS. NetScaler Gateway utiliza la dirección IP interna para comunicarse con el servidor RADIUS. Al configurar el secreto compartido, utilice la dirección IP interna. Si configura dos dispositivos para obtener alta disponibilidad, utilice la dirección IP interna virtual.
- Un secreto compartido.
- La dirección IP y el puerto del servidor SafeWord. El número de puerto predeterminado es 1812.

Para configurar la autenticación RADIUS

March 27, 2024

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. Haga clic en RADIUS y, a continuación, en el panel de detalles, en la ficha Directivas, haga clic en Agregar.
3. En el cuadro de diálogo Crear política de autenticación , en Nombre, escriba un nombre para la política.
4. En Nombre, escriba un nombre para la directiva.
5. Junto a Servidor , haz clic en Nuevo .
6. En el cuadro de diálogo Crear directiva de autenticación, en Nombre, escriba un nombre para el servidor.
7. En Servidor, en Dirección IP, escriba la dirección IP del servidor RADIUS.
8. En Puerto, escriba el puerto. El valor por defecto es 1812.
9. En Detalles, en Clave secreta y Confirmar clave secreta, escriba el secreto del servidor RADIUS.
10. En ID de NAS, escriba el número de identificador y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

Seleccionar protocolos de autenticación RADIUS

January 26, 2024

NetScaler Gateway admite implementaciones de RADIUS configuradas para utilizar varios protocolos de autenticación de usuarios, entre ellos:

- Protocolo de autenticación de contraseñas (PAP)
- Protocolo de autenticación por desafío mutuo (CHAP)
- Protocolo de autenticación Challenge Handshake de Microsoft (MS-CHAP versión 1 y versión 2)

Si la implementación de NetScaler Gateway está configurada para utilizar la autenticación RADIUS y el servidor RADIUS está configurado para usar PAP, puede reforzar la autenticación de usuarios asignando un secreto compartido fuerte al servidor RADIUS. Los secretos compartidos de RADIUS fuertes consisten en secuencias aleatorias de letras mayúsculas y minúsculas, números y signos de puntuación y tienen al menos 22 caracteres. Si es posible, utilice un programa de generación de caracteres aleatorios para determinar los secretos compartidos RADIUS.

Para proteger aún más el tráfico RADIUS, asigne un secreto compartido diferente a cada dispositivo o servidor virtual de NetScaler Gateway. Al definir clientes en el servidor RADIUS, también puede asignar un secreto compartido independiente a cada cliente. Si lo hace, debe configurar por separado cada directiva de NetScaler Gateway que utiliza la autenticación RADIUS.

Al crear una directiva RADIUS, configura secretos compartidos en NetScaler Gateway como parte de la directiva.

Configurar la extracción de direcciones IP

January 26, 2024

Puede configurar NetScaler Gateway para extraer la dirección IP de un servidor RADIUS. Cuando un usuario se autentica con el servidor RADIUS, el servidor devuelve una dirección IP enmarcada asignada al usuario. La dirección IP enmarcada también se denomina dirección IP enmarcada del atributo 8 de RADIUS en las solicitudes de acceso.

Los siguientes son componentes para la extracción de direcciones IP:

- Permite que un servidor RADIUS remoto proporcione una dirección IP de la red interna a un usuario que ha iniciado sesión en NetScaler Gateway.
- Permite la configuración de cualquier atributo RADIUS mediante el tipo **ipaddress**, incluidos los atributos codificados por proveedor.

Al configurar el servidor RADIUS para la extracción de direcciones IP, configure el identificador de proveedor y el tipo de atributo. El ID de proveedor y los atributos se utilizan para establecer la asociación entre el cliente RADIUS y el servidor RADIUS.

- El identificador de proveedor (ID) permite al servidor RADIUS asignar una dirección IP al cliente desde un grupo de direcciones IP configuradas en el servidor RADIUS. El ID de proveedor es el atributo de la respuesta RADIUS que proporciona la dirección IP de la red interna. Un valor cero indica que el atributo no está codificado por el proveedor
- El tipo de atributo es el atributo de dirección IP remota de una respuesta RADIUS. El valor mínimo es 1 y el valor máximo es 255.

Una configuración común consiste en extraer la **dirección IP enmarcada**del atributo RADIUS. El ID de proveedor está establecido en 0 o no se ha especificado. El tipo de atributo se establece en 8.

Para configurar la extracción de direcciones IP de un servidor RADIUS mediante la interfaz gráfica de usuario:

1. Vaya a **NetScaler Gateway > Directivas > Autenticación** y haga clic en **RADIUS**.
2. En el panel **Detalles**, en la ficha **Directivas**, seleccione una directiva RADIUS y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar la política de autenticación** , junto a Servidor, haga clic en **Modificar** .
4. En **Detalles**, en **Identificador de proveedor de grupo**, escriba el valor.
5. En Tipo de **atributo de grupo**, escriba el valor y, a continuación, haga clic en **Aceptar** dos veces.

Configurar la extracción de grupos RADIUS

January 26, 2024

Puede configurar la autorización RADIUS mediante un método denominado extracción de grupos. La configuración de la extracción de grupos permite administrar usuarios en el servidor RADIUS en lugar de agregarlos a NetScaler Gateway.

Para configurar la autorización RADIUS, utilice una directiva de autenticación y configure el identificador (ID) del proveedor del grupo, el tipo de atributo de grupo, el prefijo de grupo y un separador de grupos. Al configurar la directiva, agrega una expresión y, a continuación, la vincula de forma global o a un servidor virtual.

Configuración de RADIUS en Windows Server 2003

Si utiliza Microsoft Internet Authentication Service (IAS) para la autorización RADIUS en Windows Server 2003, durante la configuración de NetScaler Gateway, debe proporcionar la siguiente información:

- El identificador de proveedor es el código específico del proveedor que ha introducido en IAS.
- Type es el número de atributo asignado por el proveedor.
- Nombre de atributo es el tipo de nombre de atributo definido en IAS. El nombre predeterminado es CTXSUserGroups=

Si IAS no está instalado en el servidor RADIUS, puede instalarlo desde Agregar o quitar programas del Panel de control. Para obtener más información, consulte la Ayuda en línea de Windows.

Para configurar IAS, utilice Microsoft Management Console (MMC) e instale el complemento para IAS. Siga el asistente y asegúrese de seleccionar la siguiente configuración:

- Seleccione equipo local.
- Seleccione Directivas de acceso remoto y cree una directiva personalizada.
- Seleccione Grupos de Windows para la directiva.
- Seleccione uno de los protocolos siguientes:
  - Protocolo de autenticación por desafío mutuo de Microsoft versión 2 (MS-CHAP v2)
  - Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP)
  - Protocolo de autenticación por desafío mutuo (CHAP)
  - Autenticación sin cifrar (PAP, SPAP)
- Seleccione el atributo específico del proveedor.

  El atributo específico del proveedor debe hacer coincidir los usuarios definidos en el grupo del servidor con los usuarios de NetScaler Gateway. Para cumplir con este requisito, debe enviar los atributos específicos del proveedor a NetScaler Gateway. Asegúrese de seleccionar RADIUS=STANDARD.
- El valor predeterminado de RADIUS es 0. Utilice este número para el código de proveedor.
- El número de atributo asignado por el proveedor es 0.

  Número asignado al atributo Grupo de usuarios. El atributo está en formato de cadena.
- Seleccione Cadena para el formato de atributo.

  El valor Attribute requiere el nombre del atributo y los grupos.

  Para Access Gateway, el valor del atributo es CTXSUserGroups=groupname. Si se definen dos grupos, como ventas y finanzas, el valor del atributo es CTXSUserGroups=Sales; finance. Separe cada grupo con un punto y coma.

- Elimine todas las demás entradas del cuadro de diálogo Modificar perfil de marcado, dejando la que dice Específico del proveedor.

Después de configurar la directiva de acceso remoto en IAS, debe configurar la autenticación y autorización RADIUS en NetScaler Gateway.

Al configurar la autenticación RADIUS, utilice la configuración configurada en el servidor IAS.

Configuración de RADIUS para la autenticación en Windows Server 2008

En Windows Server 2008, se configura la autenticación y autorización RADIUS mediante el Servidor de directivas de red (NPS), que sustituye al Servicio de autenticación de Internet (IAS). Es posible utilizar el Administrador de servidores y agregar NPS como una función para instalar NPS.

Al instalar NPS, seleccione el Servicio de directivas de red. Después de la instalación, puede configurar la configuración de RADIUS para su red iniciando el NPS desde Servicios administrativos en el menú Inicio. Al abrir el NPS, agrega NetScaler Gateway como cliente RADIUS y, a continuación, configura los grupos de servidores.

Al configurar el cliente RADIUS, asegúrese de seleccionar la siguiente configuración:

- Para el nombre del proveedor, seleccione RADIUS Standard.
- Anote el secreto compartido porque tendrá que configurar el mismo secreto compartido en NetScaler Gateway.

Para los grupos RADIUS, necesita la dirección IP o el nombre de host del servidor RADIUS. No cambie la configuración predeterminada.

Después de configurar el cliente y los grupos RADIUS, configure la configuración en las dos directivas siguientes:

- Directivas de solicitud de conexión en las que se configuran los valores de la conexión de NetScaler Gateway, incluidos el tipo de servidor de red, las condiciones de la directiva de red y la configuración de la directiva.
- Directivas de red en las que se configura la autenticación del Protocolo de autenticación extensible (EAP) y los atributos específicos del proveedor.

Al configurar la directiva de solicitud de conexión, seleccione Sin especificar para el tipo de servidor de red. A continuación, configure su condición seleccionando Tipo de puerto NAS como condición y Virtual (VPN) como valor.

Al configurar una directiva de red, debe configurar los siguientes ajustes:

- Seleccione Servidor de acceso remoto (acceso telefónico VPN) como tipo de servidor de acceso a la red.

- Seleccione Autenticación cifrada (CHAP) y Autenticación sin cifrar (PAP y SPAP) para el EAP.
- Seleccione Estándar RADIUS para el atributo específico del proveedor.

  El número de atributo predeterminado es 26. Este atributo se utiliza para la autorización RADIUS.

  NetScaler Gateway necesita el atributo específico del proveedor para que los usuarios definidos en el grupo del servidor coincidan con los de NetScaler Gateway. Para ello, se envían los atributos específicos del proveedor a NetScaler Gateway.
- Seleccione Cadena para el formato de atributo.

  El valor Attribute requiere el nombre del atributo y los grupos.

  Para NetScaler Gateway, el valor del atributo es CTXSUserGroups= groupname. Si se definen dos grupos, como ventas y finanzas, el valor del atributo es CTXSUserGroups=Sales; finance. Separe cada grupo con un punto y coma.
- El separador es el que utilizó en el NPS para separar grupos, como un punto y coma, dos puntos, un espacio o un punto.

Cuando haya terminado de configurar la directiva de acceso remoto en IAS, podrá configurar la autenticación y autorización RADIUS en NetScaler Gateway.

Para configurar la autorización RADIUS

March 27, 2024

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. Haga clic en RADIUS.
3. En la ficha Directivas, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. Debajo del servidor* haga clic en +
6. En Nombre, escriba el nombre del servidor RADIUS.
7. En Servidor, escriba la dirección IP y el puerto del servidor RADIUS.
8. En Detalles, introduzca los valores de Identificador de proveedor de grupo y Tipo de atributo de grupo.
9. En Codificación de contraseña, seleccione el protocolo de autenticación y, a continuación, haga clic en Crear.
10. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione la expresión, haga clic en Agregar expresión, en Crear y, a continuación, en Cerrar.

Configurar cuentas de usuario RADIUS

March 27, 2024

NetScaler Gateway puede enviar mensajes de inicio y detención de la sesión de usuario al servidor de cuentas RADIUS. Los mensajes, que se envían para cada sesión de usuario, incluyen un subconjunto de los atributos definidos en RFC2866. En la tabla 1 se enumeran los atributos admitidos y los tipos de mensajes de cuentas RADIUS (RAD_START y RAD_STOP) en los que se envían. En la tabla 2 se enumeran los valores predefinidos que se pueden asignar al atributo `Acct-Terminate-Cause` y los eventos de NetScaler Gateway correspondientes.

Tabla 1. Atributos RADIUS compatibles

Atributo	Significado	RAD_START	RAD_STOP
User-Name	Nombre del usuario asociado a la sesión.	X	X
Session-Id	ID de sesión de NetScaler.	X	X
Acct-Session-Time	Duración de la sesión segundos.		X
Acct-Terminate-Cause	Motivo de la cancelación de la cuenta.		X

Tabla 2. Causas de la terminación

Método de cierre de sesión de NetScaler	Causa de terminación RADIUS
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST

Método de cierre de sesión de NetScaler	Causa de terminación RADIUS
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR
Otros	RAD_TERM_NAS_ERROR

La configuración de la contabilidad de usuario RADIUS requiere la creación de un par de directivas. La primera directiva es una directiva de autenticación RADIUS que designa un servidor RADIUS al que enviar mensajes de cuentas. La segunda es una directiva de sesión que utiliza la directiva de contabilidad RADIUS como acción.

Para configurar la contabilidad de usuarios RADIUS, debe:

1. Cree una directiva RADIUS para definir el servidor de cuentas RADIUS. El servidor de cuentas puede ser el mismo servidor que utiliza para la autenticación RADIUS.
2. Cree una directiva de sesión, mediante la directiva RADIUS como acción que especifica el servidor de cuentas de usuarios RADIUS.
3. Enlazar la directiva de sesión de forma global, de modo que se aplique a todo el tráfico o a un servidor virtual NetScaler Gateway, de modo que solo se aplique al tráfico que fluye a través de ese servidor virtual.

Para crear una directiva RADIUS

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Expanda Autenticación y seleccione RADI
3. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
4. Introduzca un nombre para la directiva.
5. Seleccione un servidor en el menú Servidor o haga clic en el icono + y siga las instrucciones para agregar un nuevo servidor RADIUS.
6. En el panel Expresión, en el menú Expresiones de directivas guardadas, seleccione ns_true.
7. Haga clic en Crear.

Para crear una directiva de sesión

Después de configurar una directiva RADIUS que especifica el servidor de cuentas RADIUS, cree una directiva de sesión que aplique este servidor de cuentas en una acción, como se indica a continuación:

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Selecciona Sesión .
3. En el panel de detalles principal, selecciona Agregar.
4. Introduzca un nombre para la directiva.
5. En el menú Acción, haga clic en el icono + para agregar una nueva acción de sesión.
6. Escriba un nombre para la acción de sesión.
7. Haga clic en la ficha Experiencia del cliente.
8. En el menú Directiva contable, seleccione la directiva RADIUS que creó anteriormente.
9. Haga clic en Crear.
10. En el panel Expresión, en el menú Expresiones de directivas guardadas, seleccione ns_true.
11. Haga clic en Crear.

Para enlazar la directiva de sesión de forma global

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, Directivas.
2. Selecciona Sesión .
3. En el menú Acción del panel de detalles principal, seleccione Enlaces globales.
4. Haga clic en Bind.
5. En el panel Directivas, seleccione la directiva de sesión que creó anteriormente y, a continuación, haga clic en Insertar.
6. En la lista Directivas, haga clic en la entrada Prioridad de la directiva de sesión e introduzca un valor comprendido entre 0 y 64000.
7. Haga clic en Aceptar.

Para enlazar la directiva de sesión a un servidor virtual de NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda el nodo NetScaler Gateway y, a continuación, seleccione Servidores virtuales.
2. En el panel de detalles principal, seleccione un servidor virtual y, a continuación, haga clic en Modificar.
3. En el panel Directivas, haga clic en el icono + para seleccionar una directiva.
4. En el menú Elegir directiva, seleccione Sesión y asegúrese de que la opción Solicitud esté seleccionada en el menú Elegir tipo.
5. Haga clic en Continuar.
6. Haga clic en Bind.
7. En el panel Directivas, seleccione la directiva de sesión que creó anteriormente y, a continuación, haga clic en Insertar.

8. Haga clic en Aceptar.

Configurar la autenticación SAML

March 27, 2024

El lenguaje de marcado de aserciones de seguridad (SAML) es un estándar basado en XML para intercambiar autenticación y autorización entre proveedores de identidad (IdP) y proveedores de servicios. NetScaler Gateway admite la autenticación SAML.

Al configurar la autenticación SAML, crea la siguiente configuración:

- Nombre del certificado del IdP. Esta es la clave pública que corresponde a la clave privada del IdP.
- URL de redireccionamiento. Esta es la dirección URL del IdP de autenticación. Los usuarios que no están autenticados se redirigen a esta URL.
- Campo de usuario. Puede utilizar este campo para extraer el nombre de usuario si el IdP envía el nombre de usuario en un formato diferente al de la etiqueta NameIdentifier de la etiqueta Subject. Este es un parámetro opcional.
- Nombre del certificado de firma. Es la clave privada del servidor NetScaler Gateway que se utiliza para firmar la solicitud de autenticación al IdP. Si no configura un nombre de certificado, la aserción se envía sin firmar o se rechaza la solicitud de autenticación.
- Nombre del emisor SAML. Este valor se utiliza cuando se envía la solicitud de autenticación. Debe haber un nombre único en el campo emisor para indicar la autoridad desde la que se envía la afirmación. Este campo es opcional.
- Grupo de autenticación predeterminado. Es el grupo del servidor de autenticación desde el que se autentican los usuarios.
- Dos factores. Esta configuración habilita o inhabilita la autenticación de dos factores.
- Rechazar afirmaciones sin firmar. Si se habilita, NetScaler Gateway rechaza la autenticación de usuarios si el nombre del certificado de firma no está configurado.

NetScaler Gateway admite el enlace posterior a HTTP. En este enlace, el remitente responde al usuario con 200 OK que contiene una publicación automática de formulario con la información requerida. En concreto, el formulario predeterminado debe contener dos campos ocultos llamados `SAMLRequest` y `SAMLResponse`, en función de si el formulario es una solicitud o una respuesta. El formulario también incluye RelayState, que es un estado o información utilizados por la parte remitente para enviar información arbitraria que no es procesada por una parte que confía. La parte que confía devuelve la información para que, cuando la parte remitente reciba la afirmación junto con RelayState, la parte remitente sepa qué hacer a continuación. Se recomienda cifrar u ofuscar el RelayState.

Nota

- Cuando NetScaler Gateway se usa como IdP para Citrix Cloud, no es necesario configurar la regla **RelayState** en NetScaler Gateway.
- En caso de encadenamiento de IdP, basta con configurar la regla **RelayState** solo en la primera directiva de SAML. En este contexto, el encadenamiento de IdP es un casos en el que una acción de SAML configurada hace referencia a un IdP de servidor virtual de autenticación que contiene otra acción de SAML.

Configuración de Servicios de federación de Active Directory 2.0

Puede configurar los Servicios de federación de Active Directory (AD FS) 2.0 en cualquier equipo con Windows Server 2008 o Windows Server 2012 que utilice en un rol de servidor federado. Al configurar el servidor ADFS para que sea compatible con NetScaler Gateway, debe configurar los siguientes parámetros mediante el Asistente para confianza de parte que confía en Windows Server 2008 o Windows Server 2012.

Parámetros de Windows Server 2008:

- Confianza del partido. Proporciona la ubicación del archivo de metadatos de NetScaler Gateway `https://vserver.fqdn.com/ns.metadata.xml`, por ejemplo, donde vserver.fqdn.com es el nombre de dominio completo (FQDN) del servidor virtual de NetScaler Gateway. Puede encontrar el FQDN en el certificado de servidor vinculado al servidor virtual.
- Reglas de autorización. Puede permitir o denegar a los usuarios el acceso a la parte que confía.

Parámetros de Windows Server 2012:

- Confianza del partido. Proporciona la ubicación del archivo de metadatos de NetScaler Gateway `https://vserver.fqdn.com/ns.metadata.xml`, por ejemplo, donde vserver.fqdn.com es el nombre de dominio completo (FQDN) del servidor virtual de NetScaler Gateway. Puede encontrar el FQDN en el certificado de servidor vinculado al servidor virtual.
- Perfil AD FS. Seleccione el perfil de AD FS.
- Certificado. NetScaler Gateway no admite el cifrado. No es necesario seleccionar un certificado.
- Habilite la compatibilidad con el protocolo WebSSO SAML 2.0. Esto permite admitir el inicio de sesión único de SAML 2.0. Proporciona la URL del servidor virtual de NetScaler Gateway, como `https:netScaler.virtualServerName.com/cgi/samlauth`.

  Esta URL es la URL de Assertion Consumer Service del dispositivo NetScaler Gateway. Se trata de un parámetro constante y NetScaler Gateway espera una respuesta SAML en esta URL.

- Identificador de confianza de parte que confía Escriba el nombre NetScaler Gateway. Esta es una URL que identifica a las partes que confían, por ejemplo `https://netscalerGateway.virtualServerName.com/adfs/services/trust`.
- Reglas de autorización. Puede permitir o denegar a los usuarios el acceso a la parte que confía.
- Configurar reglas de notificación. Puede configurar los valores de los atributos de LDAP mediante las reglas de transformación de emisión y la plantilla Enviar atributos de LDAP como reclamaciones. A continuación, configure los ajustes de LDAP que incluyen:
  - Direcciones de correo
  - sAMAccountName
  - Nombre principal de usuario (UPN)
  - Miembro de
- Firma de certificado. Puede especificar los certificados de verificación de firma seleccionando las propiedades de una parte retransmitiendo y, a continuación, agregando el certificado.

  Si el certificado de firma tiene menos de 2048 bits, aparece un mensaje de advertencia. Puede ignorar la advertencia para continuar. Si va a configurar una implementación de prueba, inhabilite la lista de revocación de certificados (CRL) en la parte que transmite. Si no inhabilita la comprobación, AD FS intenta la CRL para validar el certificado.

  Puede inhabilitar la CRL ejecutando el siguiente comando: Set-ADFWrelayingPartyTrust - SigningCertFicateRevocatonCheck None-TargetName NetScaler

Después de configurar la configuración, compruebe los datos de la parte que confía antes de completar el Asistente para confianza de la parte de retransmisión. Comprueba el certificado del servidor virtual de NetScaler Gateway con la URL del endpoint, como `https://vserver.fqdn.com/cgi/samlauth`.

Una vez que haya terminado de configurar los ajustes en el Asistente para confianza de la parte de retransmisión, seleccione la confianza configurada y, a continuación, modifique las propiedades. Lleve a cabo lo siguiente:

- Establezca el algoritmo hash seguro en SHA-1.

  Nota: NetScaler solo admite SHA-1.
- Elimine el certificado de cifrado. Las afirmaciones cifradas no son compatibles.
- Modifique las reglas de notificación, incluidas las siguientes:
  - Seleccionar regla de transformación
  - Agregar regla de notificación
  - Seleccionar plantilla de reglas de notificación: enviar atributos LDAP como notificaciones
  - Dar un nombre

- Seleccionar almacén de atributos: Active Directory
- Seleccione el atributo LDAP: <Active Directory parameters>
- Seleccione Regla de reclamo en marcha fuera como “ID de nombre”

Nota: Las etiquetas XML de nombre de atributo no son compatibles.

- Configure la URL de cierre de sesión para el cierre de sesión único. La regla de notificación es Enviar URL de cierre de sesión. La regla personalizada debe ser la siguiente:

```
pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs
.fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws
/2005/05/identity/claimproperties/attributename"] = "urn:oasis:
names:tc:SAML:2.0:attrname-format:unspecified"); <!--NeedCopy-->
```

Después de configurar la configuración de AD FS, descargue el certificado de firma de AD FS y, a continuación, cree una clave de certificado en NetScaler Gateway. A continuación, puede configurar la autenticación SAML en NetScaler Gateway mediante el certificado y la clave.

Configuración de la autenticación de dos factores SAML

Puede configurar la autenticación de dos factores SAML. Al configurar la autenticación SAML con autenticación LDAP, siga las siguientes pautas:

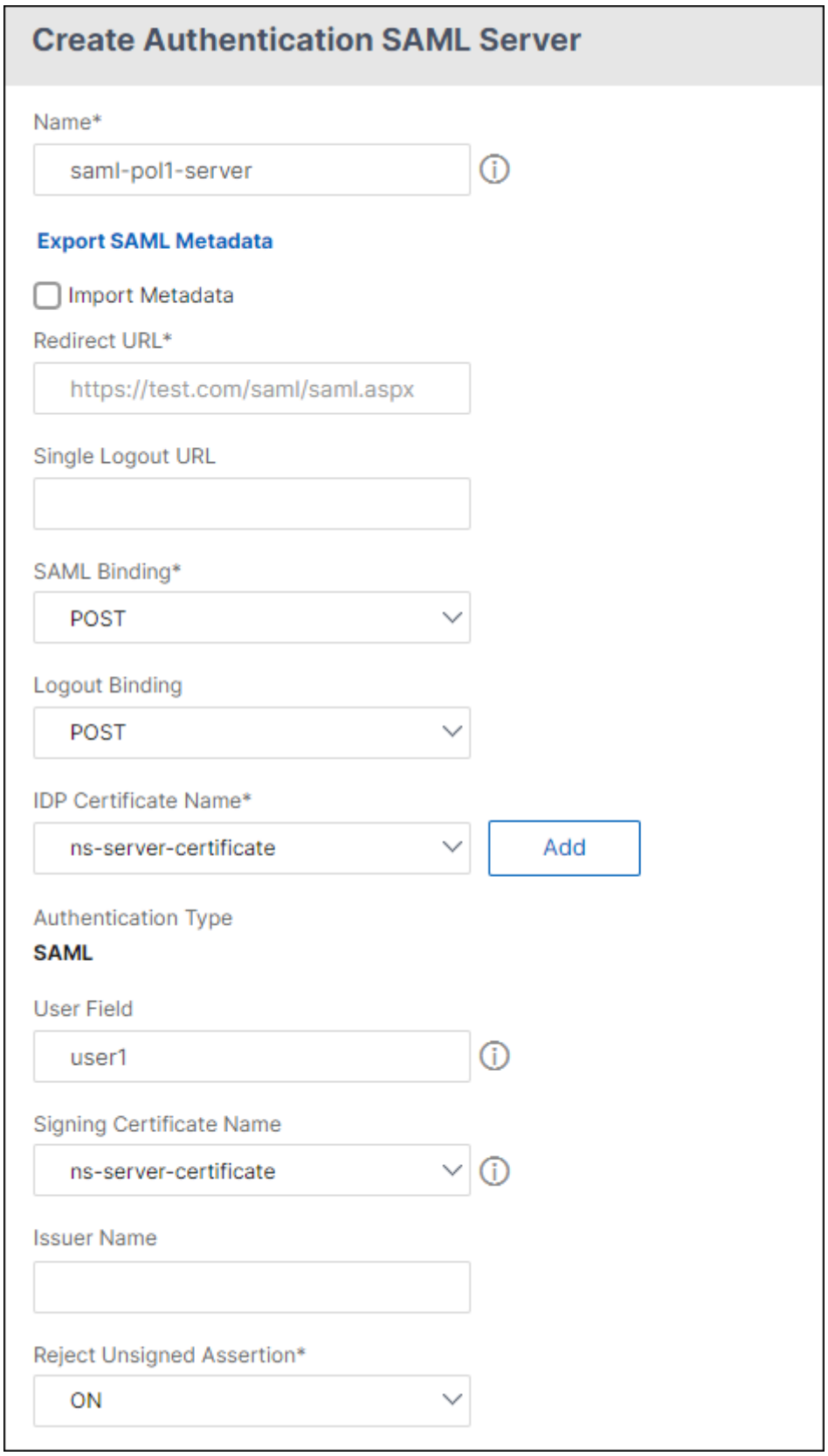
- Si SAML es el tipo de autenticación principal, inhabilite la autenticación en la directiva LDAP y configure la extracción de grupo. A continuación, vincule la directiva LDAP como tipo de autenticación secundaria.
- La autenticación SAML no utiliza una contraseña y solo utiliza el nombre de usuario. Además, la autenticación SAML solo informa a los usuarios cuando la autenticación se realiza correctamente. Si se produce un error en la autenticación SAML, no se notifica a los usuarios. Dado que no se envía una respuesta de error, SAML tiene que ser la última directiva de la cascada o la única directiva.
- Se recomienda configurar nombres de usuario reales en lugar de cadenas opacas.
- SAML no se puede enlazar como tipo de autenticación secundaria.

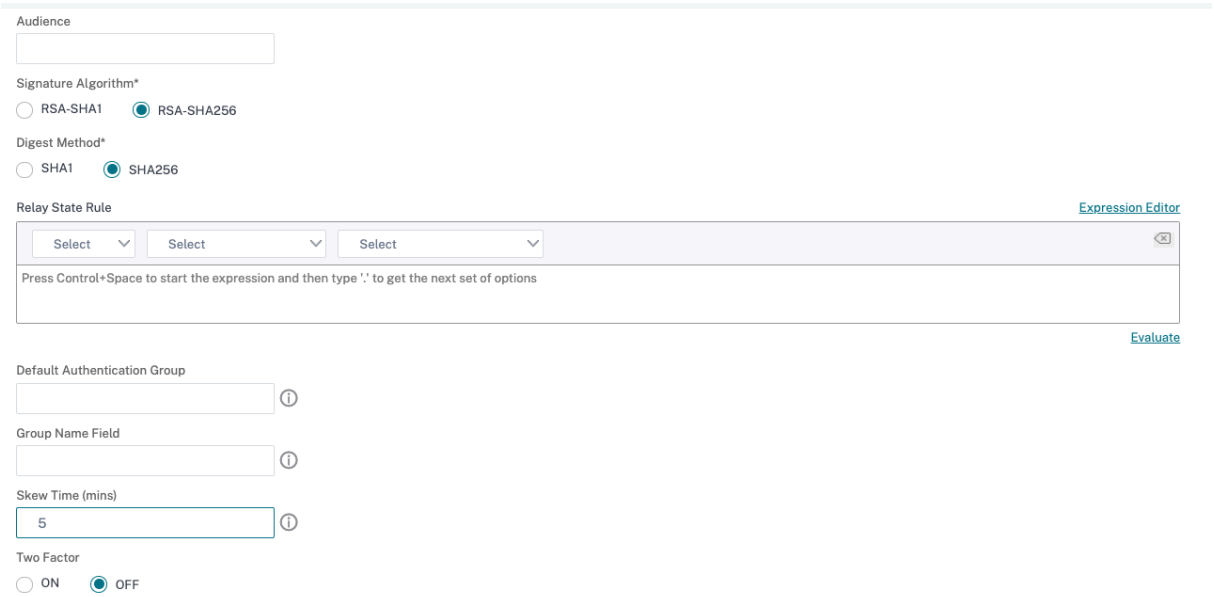
Para configurar la autenticación SAML

March 27, 2024

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.

2. En el panel de navegación, haga clic en **SAML**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo Crear directiva de autenticación, en **Nombre**, escriba un nombre para la directiva.





1. Junto a Servidor, haga clic en **Agregar**.
2. En **Nombre**, escriba un nombre para el perfil del servidor.
3. En Nombre del certificado del IdP, seleccione un certificado o haga clic en **Instalar**. Este es el certificado instalado en el servidor SAML o IdP.

   Si hace clic en Instalar, agregue el certificado y la clave privada. Para obtener más información, consulte Instalar y administrar certificados.
4. En **URL de redirección**, introduzca la URL del proveedor de identidad (IdP) de autenticación.

   Esta es la dirección URL del inicio de sesión del usuario en el servidor SAML. Este es el servidor al que NetScaler Gateway redirige la solicitud inicial.
5. En **URL de cierre de sesión único**, especifique la URL para que el dispositivo pueda reconocer cuándo debe devolver el cliente al IdP para completar el proceso de cierre de sesión.
6. En **SAML Binding**, seleccione el método que se va a utilizar para mover el cliente del SP al IdP. Esto debe ser el mismo en el IDP para que entienda cómo se conecta el cliente a él. Cuando el dispositivo actúa como SP, admite los enlaces POST, REDIRECT y ARTIFACT.
7. En **Enlace de cierre de sesión**, selecciona **REDIRECT.**
8. En **Nombre del certificado de IDP**, seleccione el certificado IdPCert (Base64) presente en el Certificado de firma SAML.

   > **Nota:**
   >
   > También puede hacer clic en **Importar metadatos** y seleccionar la URL en la que se almacena la configuración de metadatos.
9. En **Campo de usuario**, introduzca el nombre de usuario que desea extraer.

10. En **Nombre del certificado de firma**, seleccione el certificado SP SAML (con clave privada) que el dispositivo utiliza para firmar solicitudes de autenticación al IdP. El mismo certificado (sin clave privada) debe importarse al proveedor de identidades para que el proveedor de identidades pueda verificar la firma de la solicitud de autenticación. La mayoría de los desplazados internos no necesitan este campo

    Este es el certificado vinculado a la dirección IP virtual de NetScaler Gateway. El nombre del emisor SAML es el nombre de dominio completo (FQDN) en el que los usuarios inician sesión, como lb.example.com o ng.example.com.

11. En **Nombre del emisor**, introduzca el FQDN del equilibrio de carga o la dirección IP virtual de NetScaler Gateway a la que el dispositivo envía la solicitud de autenticación inicial (GET).
12. En **Rechazar aserción sin firmar**, especifique si necesita que se firmen las aserciones del IdP. Puede asegurarse de que solo la aserción debe estar firmada (activada) o que tanto la aserción como la respuesta del IdP deben estar firmadas (STRICT).
13. En **Audience**, introduzca la audiencia a la que se aplica la aserción enviada por el IdP. Normalmente se trata de un nombre de entidad o URL que representa al proveedor de servicios.
14. En **Algoritmo de firma**, seleccione RSA-SHA256
15. En **Método de resumen**, seleccione SHA256
16. En **Grupo de autenticación predeterminado**, introduzca el grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.
17. En **Nombre de grupo**, introduzca el nombre de la etiqueta en la aserción que contiene los grupos de usuarios.
18. En **Tiempo de sesgo (minutos)**, especifique la inclinación de reloj permitida en minutos que el proveedor de servicios permite en una afirmación entrante.
19. Haga clic en **Crear** y, a continuación, en **Cerrar**.
20. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione General, seleccione Valor verdadero, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Referencias

- NetScaler como SP SAML
- NetScaler como proveedor de identidades SAML
- Funciones adicionales compatibles con SAML

Usar la autenticación SAML para iniciar sesión en NetScaler Gateway

January 26, 2024

Puede utilizar la autenticación SAML para iniciar sesión en NetScaler Gateway mediante los clientes VPN y la aplicación Workspace. El complemento solo admite la autenticación SAML a través de directivas SAML avanzadas vinculadas al servidor virtual de autenticación, es decir, la autenticación nFactor.

Importante: El complemento no admite la autenticación SAML cuando las directivas SAML están enlazadas directamente al servidor virtual VPN, es decir, la autenticación no NFactor.

Plataformas y aplicaciones compatibles

En la tabla siguiente se enumeran las plataformas y aplicaciones que admiten la autenticación SAML para iniciar sesión en NetScaler Gateway.

Producto	Versión
NetScaler Gateway	Versión 12.0, compilación 41.16 y versiones posteriores
cliente VPN	Versión 12.1, compilación 49.37 y versiones posteriores. **Plataformas compatibles**: Windows 7, Windows 8, Windows 8.1, Windows 10
Versiones de la aplicación Workspace	Ventanas: 1808; Mac: 1808

Configurar la autenticación SAML mediante directivas SAML avanzadas

Para obtener más información sobre cómo configurar la autenticación SAML mediante directivas SAML avanzadas, consulte NetScaler como proveedor de identidades SAML.

Mejoras en la autenticación SAML

March 27, 2024

Esta función requiere conocimientos de SAML, conocimientos básicos de autenticación y comprensión de FIPS para utilizar esta información.

Puede utilizar las siguientes funciones de NetScaler con aplicaciones y servidores de terceros compatibles con la especificación SAML 2.0:

- Proveedor de servicios SAML (SP)
- Proveedor de identidad (IdP) SAML

El SP y el IdP permiten un inicio de sesión único (SSO) entre servicios en la nube. La función SAML SP proporciona una forma de abordar las reclamaciones de los usuarios de un IdP. El IdP puede ser un servicio de terceros u otro dispositivo NetScaler. La función de proveedor de identidades SAML se utiliza para confirmar los inicios de sesión de los usuarios y proporcionar notificaciones consumidas por los SP.

Como parte de la compatibilidad con SAML, tanto el IdP como los módulos SP firman digitalmente los datos que se envían a los pares. La firma digital incluye una solicitud de autenticación de SP, aserción del IdP y mensajes de cierre de sesión entre estas dos entidades. La firma digital valida la autenticidad del mensaje.

Las implementaciones actuales de SAML SP e IdP realizan el cálculo de firmas en un motor de paquetes. Estos módulos utilizan certificados SSL para firmar los datos. En un NetScaler compatible con FIPS, la clave privada del certificado SSL no está disponible en el motor de paquetes ni en el espacio de usuario, por lo que el módulo SAML de hoy no está preparado para hardware FIPS.

En este documento se describe el mecanismo para descargar los cálculos de firma a la tarjeta FIPS. La verificación de la firma se realiza en el software, ya que la clave pública está disponible.

Solución

El conjunto de funciones SAML se ha mejorado para utilizar una API SSL para la descarga de firmas. Consulte la documentación del producto NetScaler para obtener más información sobre estas subfunciones de SAML afectadas:

1. Enlace posterior a SAML SP: firma de AuthnRequest
2. Enlace posterior a IdP de SAML: firma de aserción/respuesta/ambos
3. Casos de cierre de sesión único de SAML SP: firma de logoutRequest en el modelo iniciado por SP y firma de LogoutResponse en el modelo iniciado por el IdP
4. Enlace de artefactos de SAML SP: firma de la solicitud ArtifactResolve
5. Enlace de redireccionamiento de SAML SP: firma de AuthnRequest
6. Enlace de redireccionamiento de IdP de SAML: firma de respuesta/aserción/ambos
7. Compatibilidad con cifrado SAML SP: descifrado de aserción

Plataforma

La API solo se puede descargar a una plataforma FIPS.

Configuración

La configuración de descarga se realiza automáticamente en la plataforma FIPS.

Sin embargo, dado que las claves privadas SSL no están disponibles para el espacio de usuario en el hardware FIPS, hay un ligero cambio de configuración al crear el certificado SSL en hardware FIPS.

Esta es la información de configuración:

- `add ssl fipsKey fips-key`

  Cree una CSR y utilícelo en el servidor de CA para generar un certificado. A continuación, puede copiar el certificado en `/nsconfig/ssl`. Supongamos que el archivo es fips3cert.cer.

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  A continuación, especifique este certificado en la acción SAML del módulo SP SAML.

- `set samlAction <name> -samlSigningCertName fips-cert`

  Del mismo modo, se utiliza en el módulo `samlIdpProfile` para el IdP de SAML.

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

La clave FIPS no está disponible la primera vez. Si no hay ninguna clave FIPS, cree una como se describe en Crear una clave FIPS.

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent
    (3 | F4)]

create certreq <reqFileName> -fipskeyName <string>
<!--NeedCopy-->
```

Configurar la autenticación TACACS+

January 26, 2024

Puede configurar un servidor TACACS+ para la autenticación. De forma similar a la autenticación RADIUS, TACACS+ utiliza una clave secreta, una dirección IP y el número de puerto. El número de puerto predeterminado es 49.

Para configurar NetScaler Gateway para que utilice un servidor TACACS+, proporcione la dirección IP del servidor y el secreto TACACS+. Debe especificar el puerto solo cuando el número de puerto del servidor en uso es algo distinto del número de puerto predeterminado de 49.

Para configurar la autenticación TACACS+ mediante la interfaz de usuario, lleve a cabo los siguientes pasos.

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.
2. Haga clic en **TACACS**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En **el campo Nombre**, escriba un nombre para la directiva.
5. Junto al campo **Servidor**, haga clic en **Agregar** para crear un nuevo servidor TACACS o haga clic en **Modificar** para realizar cambios en un servidor TACACS existente.
6. En **el campo Nombre**, escriba un nombre para el servidor.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Puerto**, utilice el número de puerto predeterminado 49.
9. En el campo **Clave TACACS**, escriba la clave. En el campo **Confirmar clave TACACS**, escriba la misma clave para confirmar.
10. Haga clic en **Más**.
11. En **Autorización**, seleccione **ACTIVADO** y, a continuación, haga clic en **Crear**.
12. En el cuadro de diálogo **Crear directiva TACACS de autenticación**, seleccione la expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Para configurar la autenticación TACACS+ mediante la interfaz de línea de comandos, escriba el siguiente comando.

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
    |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
 -tacacsSecret  }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
    auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
    defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
    Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
    Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
     [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
    string>]
<!--NeedCopy-->
```

Después de configurar la configuración del servidor TACACS+ en NetScaler Gateway, vincule la directiva para activarla. Puede enlazar la directiva a nivel de servidor global o virtual. Para obtener más información sobre las directivas de autenticación vinculantes, consulte Directivas de autenticación vinculantes.

Clear Config Basic no debe borrar la configuración TACACS

January 26, 2024

Este tema se centra en no borrar todas las configuraciones relacionadas con RBA (acceso basado en roles) cuando se ejecuta el comando clear config.

El comando clear config actual se ejecuta en uno de los tres niveles:

- Básica
- Extendida
- Completo

Según el nivel, las configuraciones de NetScaler se borran y se restablecen a los valores predeterminados de fábrica.

El comando utilizado es;

```
clear ns config [-force] <level>
<!--NeedCopy-->
```

El nuevo comando agrega un mando para permitir/denegar la eliminación de todas las configuraciones relacionadas con RBA.

Nuevo comando

Se describen las funciones de Clear RBA config:

1. Mando SÍ/NO con valor predeterminado: SÍ.

   El administrador decide si quiere conservar la configuración de RBA o no.

2. SOLO se admite el NIVEL BÁSICO de clear config.
3. Las siguientes configuraciones no se han borrado:

   - Agregar/enlazar usuario/grupo del sistema.
   - Agregar directiva cmd.
   - Comandos TACACS (agregar acción/directiva TACACS).
   - Sistema de enlace global

   Nota: La configuración relacionada con TACACS (acción/directiva) se conserva si la directiva está vinculada al sistema global o si no se borra

Configuración CLI

El comando utilizado es;

```
clear config [ – force] <level> [-RBAconfig]
<!--NeedCopy-->
```

De forma predeterminada, se establece en SÍ y borra las configuraciones según el nivel.

Si —RBAconfig se establece en NO, se conserva la configuración relacionada con RBA. Se incluye lo siguiente:

- Agregar /bind usuario del sistema /group
- Sistema de enlace global
- Comandos relacionados con TACACS (agregar acción/directiva TACACS)
- Agregar directiva cmd

Configurar la autenticación multifactor

January 26, 2024

Puede configurar dos tipos de autenticación multifactor en NetScaler Gateway:

- Autenticación en cascada que establece el nivel de prioridad de autenticación
- Autenticación de dos factores que requiere que los usuarios inicien sesión mediante dos tipos de autenticación

Si tiene varios servidores de autenticación, puede establecer la prioridad de sus directivas de autenticación. Los niveles de prioridad que establezca determinan el orden en que el servidor de autenticación valida las credenciales de los usuarios. Una directiva con un número de prioridad inferior tiene prioridad sobre una directiva con un número mayor.

Puede hacer que los usuarios se autentiquen en dos servidores de autenticación diferentes. Por ejemplo, puede configurar una directiva de autenticación LDAP y una directiva de autenticación RSA. Cuando los usuarios inician sesión, se autentican primero con su nombre de usuario y contraseña. A continuación, se autentican con un número de identificación personal (PIN) y el código del token RSA.

Configurar la autenticación en cascada

March 27, 2024

La autenticación le permite crear una cascada de varios servidores de autenticación mediante la priorización de directivas. Al configurar una cascada, el sistema atraviesa cada servidor de autenticación, según lo definido por las directivas en cascada, para validar las credenciales de un usuario. Las directivas de autenticación priorizadas se ponen en cascada en orden ascendente y pueden tener valores de prioridad comprendidos entre 1 y 9999. Defina estas prioridades al vincular sus directivas a nivel de servidor global o virtual.

Durante la autenticación, cuando un usuario inicia sesión, primero se comprueba el servidor virtual y, a continuación, se comprueban las directivas de autenticación global. Si un usuario pertenece a una directiva de autenticación tanto del servidor virtual como de forma global, la directiva del servidor virtual se aplica primero y, a continuación, la directiva de autenticación global. Si quiere que los usuarios reciban la directiva de autenticación vinculada globalmente, cambie la prioridad de la directiva. Cuando una directiva de autenticación global tiene un número de prioridad de uno y una directiva de autenticación vinculada a un servidor virtual tiene prioridad número dos, la directiva de autenticación global tiene prioridad. Por ejemplo, puede tener tres directivas de autenticación vinculadas al servidor virtual y establecer la prioridad de cada directiva.

Si un usuario no se autentica con una directiva de la cascada principal o si el usuario logra autenticarse con éxito en una directiva de la cascada principal pero no se autentica con una directiva en la cascada secundaria, el proceso de autenticación se detiene y se redirige al usuario a una página de error.

Nota: Citrix recomienda que cuando vincule varias directivas a un servidor virtual o de forma global, defina prioridades únicas para todas las directivas de autenticación.

Para establecer la prioridad de las directivas de autenticación global

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas**Autenticación.
2. Seleccione la directiva que está enlazada globalmente y, a continuación, en **Acción**, haga clic en **Enlaces globales**.
3. En el cuadro de diálogo **Vincular o desvincular directivas globales de autenticación**, en Prioridad, escriba el número y, a continuación, haga clic en **Aceptar**.

Para cambiar la prioridad de una directiva de autenticación vinculada a un servidor virtual

También puede modificar una directiva de autenticación vinculada a un servidor virtual.

1. En la utilidad de configuración, en la ficha Configuración del panel de navegación, expanda **NetScaler Gateway**y, a continuación, haga clic en Servidores **virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y haga clic en **Open**.

3. Haga clic en la ficha **Autenticación** y, a continuación, en **Primaria** o **Secundaria**
4. Junto a la directiva de autenticación, en **Prioridad**, escriba el número y, a continuación, haga clic en **Aceptar**.

Configurar la autenticación de dos factores

March 27, 2024

NetScaler Gateway admite la autenticación de dos factores. Normalmente, al autenticar usuarios, NetScaler Gateway detiene el proceso de autenticación en cuanto autentica correctamente a un usuario mediante cualquiera de los métodos de autenticación configurados. En algunos casos, es posible que necesite autenticar a un usuario en un servidor, pero extraer grupos de otro servidor. Por ejemplo, si la red autentica a los usuarios en un servidor RADIUS, pero también utiliza la autenticación de token de RSA SecurID y los grupos de usuarios se almacenan en ese servidor, es posible que deba autenticar a los usuarios en ese servidor para poder extraer los grupos.

Si los usuarios se autentican mediante dos tipos de autenticación y si uno de ellos es la autenticación de certificados de cliente, puede configurar la directiva de autenticación de certificados como segundo método de autenticación. Por ejemplo, utiliza LDAP como tipo de autenticación principal y el certificado de cliente como autenticación secundaria. Cuando los usuarios inician sesión con su nombre de usuario y contraseña, tienen acceso a los recursos de red.

Al configurar la autenticación de dos factores, selecciona si el tipo de autenticación es el tipo principal o secundario.

Para configurar la autenticación de dos factores

1. En la utilidad de configuración, en la pestaña Configuración , expanda NetScaler Gateway > Políticas Autenticación.
2. En la ficha Directivas, haga clic en Vinculaciones globales.
3. En el cuadro de diálogo Vincular o desvincular directivas de autenticación a globales, haga clic en Principal.
4. Haga clic en Insertar directiva.
5. En Nombre de directiva, seleccione la directiva de autenticación.
6. Haga clic en Secundaria, repita los pasos 4 y 5 y haga clic en Aceptar.

Seleccionar el tipo de autenticación para Single Sign-On

March 27, 2024

Si ha configurado el inicio de sesión único y la autenticación de dos factores en NetScaler Gateway, puede seleccionar qué contraseña usar para el inicio de sesión único. Por ejemplo, ha configurado LDAP como tipo de autenticación principal y RADIUS configurado como tipo de autenticación secundaria. Cuando los usuarios acceden a recursos que requieren inicio de sesión único, el nombre de usuario y la contraseña principal se envían de forma predeterminada. Establece qué contraseña se debe usar para el inicio de sesión único en aplicaciones web dentro de un perfil de sesión.

Para configurar la autenticación para el inicio de sesión único

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, haga clic en la ficha **Perfiles** y, a continuación, realice una de las siguientes acciones:
   - Para crear otro perfil, haga clic en **Agregar**.
   - Para modificar un perfil existente, haga clic en **Abrir**.
3. En la ficha Experiencia del cliente, junto a Índice de credenciales, haga clic en **Supeditación global** y seleccione **Principal** o **Secundario**.
4. Si se trata de un perfil nuevo, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
5. Si va a modificar un perfil existente, haga clic en **Aceptar**.

Configurar certificados de cliente y autenticación de dos factores LDAP

March 27, 2024

Puede utilizar un certificado de cliente seguro con autenticación y autorización LDAP, por ejemplo, mediante autenticación de tarjeta inteligente con LDAP. El usuario inicie sesión y, a continuación, se extrae el nombre de usuario del certificado de cliente. El certificado de cliente es la forma principal de autenticación y LDAP es el formulario secundario. La autenticación de certificados de cliente debe tener prioridad sobre la directiva de autenticación LDAP. Al establecer la prioridad de las directivas, asigne un número inferior a la directiva de autenticación de certificados de cliente que el número que asigna a la directiva de autenticación LDAP.

Para usar un certificado de cliente, debe tener una entidad de certificación (CA) de empresa, como Servicios de certificados de Windows Server 2008, ejecutándose en el mismo equipo que ejecuta Active Directory. Puede utilizar la entidad emisora de certificados para crear un certificado de cliente.

Para utilizar un certificado de cliente con autenticación y autorización LDAP, debe ser un certificado seguro que utilice la Secure Sockets Layer (SSL). Para utilizar certificados de cliente seguros para LDAP, instale el certificado de cliente en el dispositivo de usuario e instale el certificado raíz correspondiente en NetScaler Gateway.

Antes de configurar un certificado de cliente, haga lo siguiente:

- Cree un servidor virtual.
- Cree una directiva de autenticación LDAP para el servidor LDAP.
- Defina la expresión de la directiva LDAP en Valor verdadero.

Para configurar la autenticación de certificados de cliente con LDAP

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas\ > Autenticación**.
2. En el panel de navegación, en Autenticación, haga clic en Certificado.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre, escriba un nombre para la directiva.
5. En Tipo de autenticación, seleccione Certificado.
6. Junto a Servidor , haz clic en Nuevo .
7. En Nombre, escriba un nombre para el servidor y, a continuación, haga clic en Crear.
8. En el cuadro de diálogo Crear servidor de autenticación, en Nombre, escriba el nombre del servidor.
9. Junto a Dos factores, selecciona ON.
10. En el campo Nombre de usuario, seleccione Asunto:CN y, a continuación, haga clic en Crear.
11. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Después de crear la directiva de autenticación de certificados, enlaza la directiva al servidor virtual. Después de vincular la directiva de autenticación de certificados, vincule la directiva de autenticación LDAP al servidor virtual.

Importante: Debe enlazar la directiva de autenticación de certificados al servidor virtual antes de enlazar la directiva de autenticación LDAP al servidor virtual.

Para instalar un certificado raíz en NetScaler Gateway

Después de crear la directiva de autenticación de certificados, descarga e instala un certificado raíz de la CA en formato Base64 y lo guarda en el equipo. A continuación, puede cargar el certificado raíz en NetScaler Gateway.

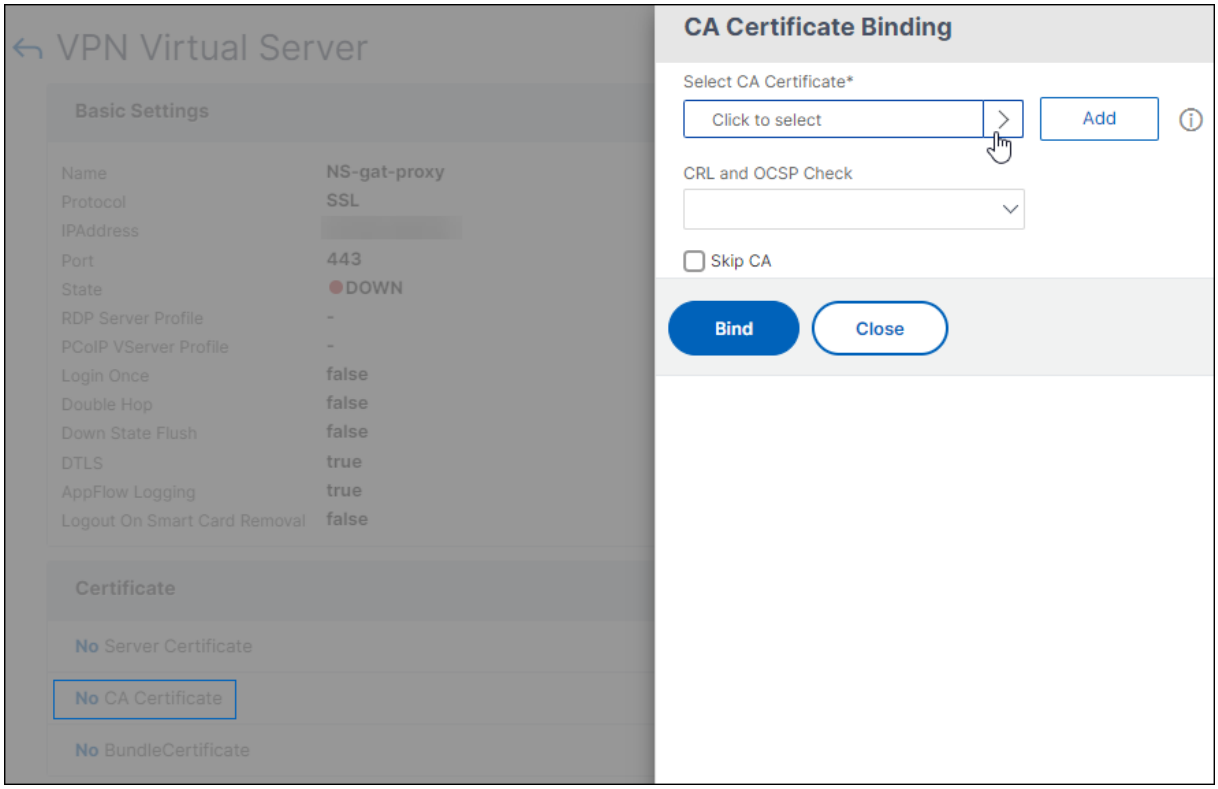
1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda SSL y, a continuación, haga clic en Certificados.
2. En el panel de detalles, haga clic en Instalar.
3. En Certificado: nombre del par de claves, escriba un nombre para el certificado.
4. En Nombre de archivo de certificado, haga clic en Examinar y, en la lista, seleccione Equipo o Local.
5. Vaya a el certificado raíz, haga clic en Abrir y, a continuación, haga clic en Instalar.

Para agregar un certificado raíz a un servidor virtual

Después de instalar el certificado raíz en NetScaler Gateway, agregue el certificado al almacén de certificados del servidor virtual.

Importante: Al agregar el certificado raíz al servidor virtual para la autenticación con tarjeta inteligente, debe seleccionar el certificado en el cuadro de lista
Seleccionar certificado de CA, como se muestra en la siguiente ilustración.

Figura 1. Agregar un certificado raíz como entidad emisora de certificados



1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En la ficha Certificados, en Disponible, seleccione el certificado, junto a Agregar, en la lista, haga clic en CA y, a continuación, haga clic en Aceptar.
4. Repita el paso 2.
5. En la ficha Certificados, haga clic en Parámetros SSL.
6. En Otros, seleccione Autenticación de cliente.
7. En Otros, junto a Certificado de cliente, seleccione Opcional y, a continuación, haga clic en Aceptar dos veces.
8. Tras configurar el certificado de cliente, pruebe la autenticación iniciando sesión en NetScaler Gateway con el cliente Citrix Secure Access. Si tiene más de un certificado instalado, recibirá un mensaje en el que se le pedirá que seleccione el certificado correcto. Después de seleccionar el certificado, aparece la pantalla de inicio de sesión con el nombre de usuario rellenado con la información obtenida del certificado. Escriba la contraseña y, a continuación, haga clic en Login.

Si no ve el nombre de usuario correcto en el campo Nombre de usuario de la pantalla de inicio de sesión, compruebe las cuentas de usuario y los grupos del directorio LDAP. Los grupos definidos en

NetScaler Gateway deben ser los mismos que los del directorio LDAP. En Active Directory, configure grupos en el nivel raíz del dominio. Si crea grupos de Active Directory que no están en el nivel raíz del dominio, puede producirse una lectura incorrecta del certificado de cliente.

Si los usuarios y los grupos no están en el nivel raíz del dominio, la página de inicio de sesión de NetScaler Gateway muestra el nombre de usuario configurado en Active Directory. Por ejemplo, en Active Directory, tiene una carpeta denominada Usuarios y el certificado dice CN=Usuarios. En la página de inicio de sesión, en Nombre de usuario, aparece la palabra Usuarios.

Si no quiere mover sus cuentas de grupo y usuario al nivel de dominio raíz, cuando configure el servidor de autenticación de certificados en NetScaler Gateway, deje en blanco el campo de nombre de usuario y el campo de nombre de grupo.

Configurar Single Sign-On

January 26, 2024

Puede configurar NetScaler Gateway para que admita el inicio de sesión único con Windows, aplicaciones web (como SharePoint), recursos compartidos de archivos y la Interfaz Web. El inicio de sesión único también se aplica a los recursos compartidos de archivos a los que los usuarios pueden acceder mediante la utilidad de transferencia de archivos de la interfaz de acceso o desde el menú de iconos de NetScaler Gateway en el área de notificación.

Si configura el inicio de sesión único cuando los usuarios inician sesión, vuelven a iniciar sesión automáticamente sin tener que introducir sus credenciales por segunda vez.

Configurar Single Sign-On con Windows

March 27, 2024

Los usuarios abren una conexión iniciando el cliente Citrix Secure Access desde el escritorio. Puede especificar que el cliente Citrix Secure Access se inicie automáticamente cuando el usuario inicie sesión en Windows habilitando el inicio de sesión único. Al configurar el inicio de sesión único, las credenciales de inicio de sesión de Windows de los usuarios se transfieren a NetScaler Gateway para su autenticación. Al habilitar el inicio de sesión único para el cliente Citrix Secure Access, se facilitan las operaciones en el dispositivo del usuario, como los scripts de instalación y la asignación automática de unidades.

Habilita el inicio de sesión único solo si los dispositivos de usuario inician sesión en el dominio de su organización. Si el inicio de sesión único está habilitado y un usuario se conecta desde un dispositivo

que no está en su dominio, se le pedirá al usuario que inicie sesión.

El inicio de sesión único se configura con Windows de forma global o mediante un perfil de sesión asociado a una directiva de sesión.

Para configurar el inicio de sesión único con Windows de forma global

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, haga clic en Inicio de **sesión único con Windows**y, a continuación, haga clic en **Aceptar**.

Para configurar el inicio de sesión único con Windows mediante una directiva de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. **Junto a Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, junto a Inicio de **sesión único con Windows, haga clic en-Sobrescribir global**, haga clic**en Inicio de sesión único con Windows**y, a continuación, haga clic en**Aceptar**.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione Valor verdadero, haga clic en **Agregar expresión**, en **Crear**y, a continuación, en **Cerrar**.

Configuración de Single Sign-On en Aplicaciones web

March 27, 2024

Puede configurar NetScaler Gateway para proporcionar inicio de sesión único a los servidores de la red interna que utilizan autenticación basada en web. Con el inicio de sesión único, puede redirigir al usuario a una página principal personalizada, como un sitio de SharePoint o a la Interfaz Web. También puede configurar el inicio de sesión único en los recursos a través del cliente Citrix Secure Access desde un marcador configurado en la página principal o una dirección web que los usuarios escriban en el navegador web.

Si va a redirigir la página principal a un sitio de SharePoint o a una Interfaz Web, proporcione la dirección web del sitio. Cuando los usuarios se autentican, ya sea mediante NetScaler Gateway o un servidor de autenticación externo, los usuarios se redirigen a la página principal especificada. Las credenciales de usuario se transfieren de forma transparente al servidor web. Si el servidor web acepta las credenciales, los usuarios inician sesión automáticamente. Si el servidor web deniega las credenciales, los usuarios reciben un mensaje de autenticación en el que se les pide su nombre de usuario y contraseña.

Puede configurar el inicio de sesión único en aplicaciones web de forma global o mediante una directiva de sesión.

Para configurar el inicio de sesión único en aplicaciones web de forma global

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, haga clic en Inicio de sesión único en aplicaciones web y, a continuación, haga clic en Aceptar.

Para configurar el inicio de sesión único en aplicaciones web mediante una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway > Políticas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la ficha Directivas, seleccione una directiva de sesión y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar política de sesión , junto a Solicitar perfil , haga clic en Modificar .
4. En la ficha Experiencia del cliente, junto a Inicio de sesión único en aplicaciones web, haga clic en Invalidación global, haga clic en Inicio de sesión único en aplicaciones web y, a continuación, haga clic en Aceptar.

Para definir el puerto HTTP para Single Sign-On en aplicaciones web

El inicio de sesión único solo se intenta para el tráfico de red en el que el puerto de destino se considera un puerto HTTP. Para permitir el inicio de sesión único en aplicaciones que utilizan un puerto distinto del puerto 80 para el tráfico HTTP, agregue uno o varios números de puerto en NetScaler Gateway. Puede habilitar varios puertos. Los puertos se configuran globalmente.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Configuración de red, haga clic en Configuración avanzada.
4. En Puertos HTTP, escriba el número de puerto, haga clic en Agregar y, a continuación, haga clic en Aceptar dos veces.

   Puede repetir el paso 4 para cada puerto que quiera agregar.

Nota: Si las aplicaciones web de la red interna utilizan direcciones IP públicas, el inicio de sesión único no funciona. Para habilitar el inicio de sesión único, se debe habilitar la tunelización dividida como parte de la configuración de la directiva global, independientemente de si se utiliza el acceso sin cliente o el cliente Citrix Secure Access para las conexiones de los dispositivos de usuario. Si no es posible habilitar la tunelización dividida a nivel global, cree un servidor virtual que utilice un intervalo de direcciones privadas.

Configuración del inicio de sesión único en aplicaciones web mediante LDAP

March 27, 2024

Cuando configura el inicio de sesión único y los usuarios inician sesión con el nombre principal de usuario (UPN) con el formato username@domain.com, el inicio de sesión único falla de forma predeterminada y los usuarios deben autenticarse dos veces. Si necesita utilizar este formato para el inicio de sesión de usuario, modifique la directiva de autenticación LDAP para aceptar esta forma de nombre de usuario.

Para configurar el inicio de sesión único en aplicaciones web

1. En la utilidad de configuración, en la pestaña **Configuración** , expanda **NetScaler Gateway > Políticas Autenticación**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva LDAP y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar la directiva de autenticación**, junto a **Servidor**, haga clic en **Modificar**.
4. En **Configuración de conexión**, en DN base (ubicación de los usuarios), escriba DC=nombredominio, DC=com.

5. En **Administrator Vincular DN**, escriba LDAPaccount@domainname.com, donde nombredominio.com es el nombre de su dominio.
6. En **Contraseña** de **administrador y Confirmar contraseña**de administrador, escriba la contraseña.
7. En **Otra configuración**, en **Atributo de nombre de inicio de sesión del servidor**, escriba UserPrincipalName.
8. En **Atributo de grupo**, escriba memberOf.
9. En **Nombre de subatributo**, escriba CN.
10. En **Atributo de nombre de SSO**, escriba el formato con el que los usuarios inician sesión y, a continuación, haga clic en **Aceptar** dos veces. Este valor es `SamAccountName` o `UserPrincipalName`.

Configurar Single Sign-On en un dominio

March 27, 2024

Si los usuarios se conectan a servidores que ejecutan Citrix Virtual Apps y utilizan SmartAccess, puede configurar el inicio de sesión único para los usuarios que se conectan a la comunidad de servidores. Cuando configure el acceso a aplicaciones publicadas mediante una directiva y un perfil de sesión, utilice el nombre de dominio para la comunidad de servidores.

También puede configurar el inicio de sesión único para compartir archivos en la red.

Para configurar el inicio de sesión único en un dominio

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway > Políticas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la ficha Directivas, seleccione una directiva de sesión y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configurar política de sesión , junto a Solicitar perfil , haga clic en Modificar .
4. En el cuadro de diálogo Configurar perfil de sesión, en la ficha Aplicaciones publicadas, en Dominio de inicio de sesión único, haga clic en Supeditación global, escriba el nombre del dominio y, a continuación, haga clic en Aceptar dos veces.

Para obtener más información sobre cómo configurar NetScaler Gateway con Citrix Virtual Apps, consulte Integración de NetScaler Gateway con Citrix Virtual Apps and Desktops.

Configuración del inicio de sesión único para Microsoft Exchange 2010

January 26, 2024

En la siguiente sección se describe la configuración del inicio de sesión único (SSO) para Microsoft Exchange 2010 en NetScaler Gateway. El SSO de Outlook Web Access (OWA) 2010 no funciona en las siguientes condiciones:

- Uso de la autenticación basada en formularios en Microsoft Exchange 2010.
- Servidor virtual de equilibrio de carga con directiva de administración del tráfico de autenticación, autorización y auditoría.

> **Nota:** Esta configuración solo funciona para servidores virtuales de equilibrio de carga con directiva de administración de tráfico de autenticación, autorización y auditoría. No funciona para el SSO en OWA 2010 con VPN sin cliente.

Los siguientes pasos son requisitos previos que debe tener en cuenta antes de configurar el inicio de sesión solo para Microsoft Exchange 2010 en NetScaler Gateway.

- El formulario URL de acción para SSO es diferente en OWA 2010. Modifique la directiva de administración del tráfico en consecuencia.
- Necesita una directiva de reescritura para configurar la cookie `PBack` en la solicitud logon.aspx. En situaciones normales, establezca la cookie `PBack` en el cliente y haga clic en Enviar.
- Cuando utiliza SSO, se consume la respuesta a logon.aspx y NetScaler Gateway genera la solicitud de formulario. La cookie no se adjunta en la solicitud de envío del formulario.
- El servidor de OWA espera la cookie `PBack` en la solicitud de envío del formulario. La directiva de reescritura es necesaria para adjuntar la cookie `PBack` en la solicitud de envío del formulario.

Realice lo siguiente mediante la CLI

1. Configurar la administración del tráfico de autenticación, autorización y auditoría

   ```
   add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.
   owa"-userField username -passwdField password -ssoSuccessRule "
   http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.
   GT(70"-responsesize 15000 -submitMethod POST
   ```

2. Configure la directiva de administración del tráfico y vincule la directiva

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`

- `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
- `bind tm global -policyName owa2k10_pol -priority 100`

Reescritura de configuración mediante CLI

En la línea de comandos, escriba:

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

Configuración de reescritura alternativa

En raras ocasiones, es posible que Microsoft Outlook no emita cookies de sesión de OWA y que las cookies `Pback` tampoco se inserten. El problema puede producirse después de ejecutar los comandos anteriores para implementar la configuración de reescritura.

Para superar estos casos y como solución alternativa, puede configurar los siguientes comandos en lugar de la configuración de reescritura.

En la línea de comandos, escriba:

- `add rewrite action set_pback_cookie insert_http_header "Cookie"'" PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

Configurar el uso único de la contraseña

January 26, 2024

Puede configurar NetScaler Gateway para que utilice contraseñas de un solo uso, como un número de identificación personal (PIN) de token o un código de acceso. Una vez que un usuario introduce el

código de acceso o el PIN, el servidor de autenticación invalida inmediatamente la contraseña de un solo uso y el usuario no puede volver a introducir el mismo PIN o contraseña.

Los productos que incluyen el uso de una contraseña de un solo uso incluyen:

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

Para utilizar cada uno de estos productos, configure el servidor de autenticación de la red interna para que utilice RADIUS. Para obtener más información, consulte Configuración de la autenticación RADIUS.

Si configura la autenticación en NetScaler Gateway para que utilice una contraseña de un solo uso con RADIUS, tal como lo proporciona un token de RSA SecurID, por ejemplo, NetScaler Gateway intenta volver a autenticar a los usuarios mediante la contraseña almacenada en caché. Esta reautenticación se produce cuando se realizan cambios en NetScaler Gateway o si la conexión entre el cliente Citrix Secure Access y NetScaler Gateway se interrumpe y, a continuación, se restablece.

También se puede intentar volver a autenticarse cuando las conexiones se configuran para usar la aplicación Citrix Workspace y los usuarios se conectan a la Interfaz Web mediante RADIUS o LDAP. Cuando un usuario inicia una aplicación y la usa y, a continuación, vuelve a Receiver para iniciar otra aplicación, NetScaler Gateway utiliza la información almacenada en caché para autenticar al usuario.

Configurar RSA SecurID Authentication

January 26, 2024

Al configurar el servidor RSA/ACE para la autenticación RSA SecureID, debe completar los siguientes pasos:

Configure el cliente RADIUS con la siguiente información:

- Proporcione el nombre del dispositivo NetScaler Gateway.
- Proporciona una descripción (no es obligatorio).
- Proporcione la dirección IP del sistema.
- Proporcione el secreto compartido entre NetScaler Gateway y el servidor RADIUS.
- Configure la marca/modelo como RADIUS estándar.

En la configuración del host del agente, necesita la siguiente información:

- Proporcione el nombre de dominio completo (FQDN) de NetScaler Gateway (tal y como aparece en el certificado vinculado al servidor virtual). Después de proporcionar el FQDN, haga clic en la tecla Tabulador y se rellenará la ventana Dirección de red.

  Después de introducir el FQDN, la dirección de red aparece automáticamente. Si no lo hace, introduzca la dirección IP del sistema.
- Proporcione el tipo de agente mediante Communication Server.
- Configúrelo para importar todos los usuarios o un conjunto de usuarios a los que se les permite autenticarse a través de NetScaler Gateway.

Si aún no está configurada, cree una entrada Host de agente para el servidor RADIUS, que incluya la siguiente información:

- Proporcione el FQDN del servidor RSA.

  Después de introducir el FQDN, la dirección de red aparece automáticamente. Si no es así, proporcione la dirección IP del servidor RSA.
- Proporcione el tipo de agente, que es el servidor RADIUS.

Para obtener más información sobre la configuración de un servidor RADIUS RSA, consulte la documentación del fabricante.

Para configurar RSA SecurID, cree un perfil y una directiva de autenticación y, a continuación, vincule la directiva de forma global o a un servidor virtual. Para crear una directiva RADIUS para utilizar RSA SecurID, consulte Configuración de la autenticación RADIUS.

Después de crear la directiva de autenticación, enlaza la directiva a un servidor virtual o de forma global. Para obtener más información, consulte Directivas de autenticación vinculantes.

Configurar la devolución de contraseña con RADIUS

January 26, 2024

Puede reemplazar las contraseñas de dominio por una contraseña de un solo uso que genera un token desde un servidor RADIUS. Cuando los usuarios inician sesión en NetScaler Gateway, introducen un número de identificación personal (PIN) y el código de acceso del token. Una vez que NetScaler Gateway valida sus credenciales, el servidor RADIUS devuelve la contraseña de Windows del usuario a NetScaler Gateway. NetScaler Gateway acepta la respuesta del servidor y, a continuación, utiliza la contraseña devuelta para el inicio de sesión único en lugar de utilizar el código de acceso que los usuarios escribían durante el inicio de sesión. Esta devolución de contraseña con la función RADIUS permite configurar el inicio de sesión único sin que los usuarios tengan que recuperar su contraseña de Windows.

Cuando los usuarios inician sesión con la devolución de contraseña, pueden acceder a todos los recursos de red permitidos en la red interna, incluidos Citrix Endpoint Management, StoreFront y la interfaz web.

Para habilitar el inicio de sesión único mediante contraseñas devueltas, configure una directiva de autenticación RADIUS en NetScaler Gateway mediante los parámetros Identificador de proveedor de contraseña y Tipo de atributo de contraseña. Estos dos parámetros devuelven la contraseña de Windows del usuario a NetScaler Gateway.

NetScaler Gateway admite Imprivata OneSign. La versión mínima requerida de Imprivata OneSign es 4.0 con service pack 3. El identificador de proveedor de contraseñas predeterminado para Imprivata OneSign es 398. El código de tipo de atributo de contraseña predeterminado para Imprivata OneSign es 5.

Puede utilizar otros servidores RADIUS para devolver contraseñas, como RSA, Cisco o Microsoft. Configure el servidor RADIUS para que devuelva la contraseña de inicio de sesión único del usuario en un par de valores de atributos específicos del proveedor. En una directiva de autenticación de NetScaler Gateway, debe agregar los parámetros **Identificador de proveedor de contraseña y** Tipo de atributo de contraseña para estos servidores.

Puede encontrar una lista completa de identificadores de proveedores en el sitio web de la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, el identificador de proveedor para la seguridad RSA es 2197, para Microsoft es 311 y para Cisco Systems es 9. El atributo específico del proveedor que admite un proveedor debe confirmarse con el proveedor. Por ejemplo, Microsoft ha publicado una lista de atributos específicos del proveedor en Atributos RADIUS específicos del proveedor de Microsoft.

Puede seleccionar cualquiera de los atributos específicos del proveedor para almacenar la contraseña de inicio de sesión único de los usuarios en el servidor RADIUS del proveedor. Si configura NetScaler Gateway con el identificador de proveedor y el atributo donde se almacena la contraseña de usuario en el servidor RADIUS, NetScaler Gateway solicita el valor del atributo en el paquete de solicitud de acceso que se envía al servidor RADIUS. Si el servidor RADIUS responde con el par atributo-valor correspondiente en el paquete de aceptación de acceso, la devolución de contraseña funciona independientemente del servidor RADIUS que utilice.

Para configurar el inicio de sesión único mediante contraseñas devueltas:

1. En la utilidad de configuración, en la ficha Configuración, expanda **NetScaler Gateway > Directivas\ > Autenticación**.
2. En el panel de navegación, haga clic en **RADIUS**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo **Crear política de autenticación** , en Nombre, escriba un nombre para la política.
5. Junto a **Servidor** , haz clic en **Nuevo** .

6. En **Nombre**, escriba el nombre del servidor.
7. Configure los ajustes del servidor RADIUS.
8. En **Identificador de proveedor de contraseña**, escriba el identificador de proveedor que devuelve el servidor RADIUS. Este identificador debe tener un valor mínimo de 1.
9. En **Tipo de atributo de contraseña**, escriba el tipo de atributo que devuelve el servidor RADIUS en el código AVP específico del proveedor. El valor puede oscilar entre 1 y 255.
10. En el cuadro de diálogo **Crear directiva de autenticación** , junto a **Expresiones con nombre** , seleccione la expresión, haga clic en **Agregar expresión** , en **Crear** y, a continuación, en **Cerrar** .

Configurar la autenticación de SafeWord

January 26, 2024

La línea de productos SafeWord ayuda a proporcionar una autenticación segura mediante el uso de un código de acceso basado en tokens. Una vez que los usuarios introducen un código de acceso, SafeWord lo invalida y no se puede volver a utilizar.

Si Access Gateway sustituye a Secure Gateway en una implementación de Secure Gateway e Interfaz Web, puede optar por no configurar la autenticación en Access Gateway y seguir permitiendo que la interfaz web proporcione autenticación de SafeWord para el tráfico HTTP entrante.

Access Gateway admite la autenticación SafeWord para los siguientes productos:

- SafeWord 2008
- Acceso a SafeWord Premier
- SafeWord para Citrix
- Acceso remoto SafeWord

Puede configurar Access Gateway para que se autentique mediante productos SafeWord de las siguientes maneras:

- Configure la autenticación para utilizar un servidor RADIUS de PremierAccess instalado como parte de SafeWord PremierAccess y permita que gestione la autenticación.
- Configure la autenticación para utilizar el agente IAS de SafeWord, que es un componente de SafeWord RemoteAccess, SafeWord para Citrix y SafeWord PremierAccess 4.0.
- Instale el agente de interfaz web de SafeWord para admitir la interfaz web de Citrix. No es necesario configurar la autenticación en Access Gateway y la interfaz web de Citrix puede gestionarlo. Esta configuración no utiliza el servidor RADIUS de PremierAccess ni el agente IAS de SafeWord.

Al configurar el servidor RADIUS de SafeWord, necesita la siguiente información:

- Dirección IP de Access Gateway. Al configurar la configuración del cliente en el servidor RADIUS, utilice la dirección IP de Access Gateway.
- Un secreto compartido.
- La dirección IP y el puerto del servidor SafeWord.

Configurar la autenticación de Gemalto Protiva

January 26, 2024

Protiva es una plataforma de autenticación sólida que se desarrolló para utilizar los puntos fuertes de la autenticación con tarjeta inteligente de Gemalto. Con Protiva, los usuarios inician sesión con un nombre de usuario, una contraseña y una contraseña de un solo uso generados por el dispositivo Protiva. Al igual que RSA SecurID, la solicitud de autenticación se envía al servidor de autenticación de Protiva y la contraseña se valida o se rechaza.

Para configurar Gemalto Protiva para que sea compatible con NetScaler Gateway, siga las siguientes pautas:

- Instale el servidor Protiva.
- Instale el complemento del agente Protiva Internet Authentication Server (IAS) en un servidor RADIUS de Microsoft IAS. Asegúrese de anotar la dirección IP y el número de puerto del servidor IAS.

nFactor para autenticación de puerta de enlace

March 27, 2024

La autenticación nFactor permite un conjunto completamente nuevo de posibilidades en relación con la autenticación. Los administradores que utilizan nFactor disfrutan de flexibilidad de autenticación, autorización y auditoría al configurar factores de autenticación para servidores virtuales.

Dos bancos de directivas o dos factores ya no restringen a un administrador. El número de bancos de directivas puede ampliarse para adaptarse a diferentes necesidades. En función de factores anteriores, nFactor determina un método de autenticación. Los formularios de inicio de sesión dinámicos y las acciones en caso de fallo son posibles mediante nFactor.

> **Importante**
>
> - A partir de la versión 13.0, compilación 67.x, la autenticación nFactor solo se admite con

> la licencia estándar para el servidor virtual Gateway/VPN, y no para el servidor virtual de autenticación. En la licencia estándar, la GUI del visualizador nFactor no se puede utilizar para crear EPA en el flujo nFactor. Además, no puede modificar el esquema de inicio de sesión, pero debe usar el esquema de inicio de sesión listo para usar tal cual.
> - Para que NetScaler admita la autenticación nFactor, se necesita una licencia Advanced o Premium. Para obtener más información sobre la autenticación nFactor con NetScaler, consulte Autenticación nFactor.

Requisitos de licencia de funciones de autenticación, autorización y auditoría

En la siguiente tabla se enumeran los requisitos de licencia para las funciones de autenticación, autorización y auditoría disponibles.

	Licencia estándar	Licencia avanzada	Licencia premium
Autentificación LOCAL	Sí	Sí	Sí
Autenticación LDAP	Sí	Sí	Sí
Autenticación RADIUS	Sí	Sí	Sí
Autenticación TACACS	Sí	Sí	Sí
Autentificación web	Sí	Sí	Sí
Autenticación de certificados cliente	Sí	Sí	Sí
Negociar la autenticación	Sí	Sí	Sí
Autenticación SAML	Sí	Sí	Sí
Autenticación OAuth	No	Sí	Sí
OTP nativo	No	Sí	Sí

		Licencia estándar	Licencia avanzada	Licencia premium
	Correo electrónico OTP	No	Sí	Sí
	Notificación push para OTP	No	No	Sí
	Preguntas y respuestas basadas en el conocimiento (autenticación KBA)	No	Sí	Sí
	Restablecimiento de contraseña de autoservicio (SSPR)	No	Sí	Sí
	Visualizador nFactor	Sí	Sí	Sí

Nota

- Para obtener los pasos para configurar nFactor para la licencia estándar de NetScaler, consulte la sección Crear un servidor virtual de puerta de enlace para la autenticación nFactor en la licencia estándar de NetScaler.
- Solo un servidor virtual de autenticación, autorización y auditoría no direccionable se puede vincular a un servidor virtual de puerta de enlace o VPN en la licencia NetScaler Standard.
- La personalización de LoginSchema no está permitida en la licencia NetScaler Standard. La compatibilidad con nFactor es básica, con esquemas de inicio de sesión predeterminados y ya agregados que vienen con el dispositivo. El administrador puede utilizarlos en sus configuraciones, pero no puede agregar un esquema de inicio de sesión. Por lo tanto, la opción GUI está inhabilitada.

Casos de uso

La autenticación nFactor permite flujos de autenticación dinámicos basados en el perfil de usuario. En ocasiones, los flujos pueden ser sencillos e intuitivos para el usuario. En otros casos, se pueden

combinar con la protección de active directory u otros servidores de autenticación. A continuación se indican algunos requisitos específicos de Gateway:

1. **Selección dinámica de nombre de usuario y contraseña.** Tradicionalmente, los clientes (incluidos los exploradores web y los Receivers) utilizan la contraseña de Active Directory (AD) como primer campo de contraseña. La segunda contraseña está reservada para la contraseña de un solo tiempo (OTP). Sin embargo, para proteger los servidores de AD, es necesario validar primero OTP. nFactor puede hacerlo sin necesidad de modificaciones del cliente.
2. **Punto final de autenticación multiarrendatario.** Algunas organizaciones utilizan distintos servidores de puerta de enlace para usuarios certificados y no certificados. Dado que los usuarios utilizan sus propios dispositivos para iniciar sesión, los niveles de acceso de los usuarios varían según el dispositivo NetScaler en función del dispositivo que se esté mediante. Gateway puede satisfacer diferentes necesidades de autenticación.
3. **Autenticación basada en la pertenencia a un grupo.** Algunas organizaciones obtienen propiedades de usuario de los servidores de AD para determinar los requisitos de autenticación. Los requisitos de autenticación pueden variar para cada usuario.
4. **Cofactores de autenticación.** En ocasiones, se utilizan diferentes pares de directivas de autenticación para autenticar distintos conjuntos de usuarios. La provisión de directivas de pares aumenta la autenticación efectiva. Las directivas dependientes se pueden crear a partir de un flujo. De esta manera, los conjuntos de directivas independientes se convierten en flujos propios que aumentan la eficiencia y reducen la complejidad.

Gestión de respuestas de autenticación

Los registros de devolución de llamada de NetScaler Gateway gestionan las respuestas de autenticación. Las respuestas AAAD (daemon de autenticación) y los códigos de éxito/fallo/error/diálogo se alimentan al gestor de devolución de llamada. Los códigos de éxito/fracaso/error/diálogo dirigen a Gateway a tomar las medidas adecuadas.

Soporte al cliente

En la tabla siguiente se detallan los detalles de configuración.

Cliente	Soporte nFactor	Punto de enlace de directiva de autenticación	EPA
Exploradores web	Sí	Autenticación	Sí

Cliente	Soporte nFactor	Punto de enlace de directiva de autenticación	EPA
Aplicación Citrix Workspace	Sí	VPN	Sí
Plug-in de Gateway	Sí	VPN	Sí

Nota:

- La aplicación Citrix Workspace admite la autenticación nFactor para los sistemas operativos compatibles de las siguientes versiones de la lista.
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: compatible con Store Web
  - Chrome: compatible con Store Web

Configuración de línea de comandos

El servidor virtual de puerta de enlace necesita un servidor virtual de autenticación denominado como atributo. El nombre del servidor virtual como atributo es la única configuración necesaria para este modelo.

```
1 add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
2 <!--NeedCopy-->
```

authnVsName es el nombre del servidor virtual de autenticación. El servidor virtual authnVsName debe configurarse con directivas de autenticación avanzadas y se utiliza para la autenticación nFactor.

```
1 add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
     -profile>
2 set vpn vserver <name> -authnProfile <name-of-profile>
3 <!--NeedCopy-->
```

Donde authnProfile es el perfil de autenticación creado anteriormente.

Retos de interoperabilidad

La mayoría de los clientes de Legacy Gateway, además de los clientes rfWeb, se modelan según las respuestas enviadas por Gateway. Por ejemplo, se espera una respuesta 302 a /vpn/index.html para muchos clientes. Estos clientes también dependen de varias cookies de puerta de enlace, como "pwcount", "NSC_CERT".

Análisis de puntos finales (EPA)

EPA en nFactor no es compatible con el módulo de autenticación, autorización y auditoría de NetScaler. Por lo tanto, el servidor virtual de NetScaler Gateway lleva a cabo EPA. Después de EPA, las credenciales de inicio de sesión se envían al servidor virtual de autenticación mediante la API mencionada anteriormente. Una vez finalizada la autenticación, Gateway continúa con el proceso posterior a la autenticación y establece la sesión del usuario.

Consideraciones sobre configuraciones erróneas

El cliente Gateway envía las credenciales de usuario solo una vez. Gateway obtiene una o dos credenciales del cliente con la solicitud de inicio de sesión. En el modo heredado, hay un máximo de dos factores. Las contraseñas obtenidas se utilizan para estos factores. Sin embargo, con nFactor el número de factores que se pueden configurar es prácticamente ilimitado. Las contraseñas obtenidas del cliente Gateway se reutilizan (según la configuración) para los factores configurados. Se debe tener cuidado de que la contraseña de un solo uso (OTP) no se vuelva a utilizar varias veces. Del mismo modo, un administrador debe asegurarse de que la contraseña reutilizada en un factor sea aplicable a ese factor.

Definición de clientes

La opción de configuración se proporciona para ayudar a NetScaler a determinar los clientes del explorador en comparación con los clientes pesados como Receiver.

Se proporciona un conjunto de patrones, ns_vpn_client_useragents, para que el administrador configure los patrones para todos los clientes.

Del mismo modo, vincular la cadena "Citrix Receiver"al `patset` anterior para ignorar todos los clientes que tengan "Citrix Receiver"en el user-Agent.

Restricción de nFactor para Gateway

nFactor para autenticación de puerta de enlace no se produce si se dan las siguientes condiciones.

1. authnProfile no está establecido en NetScaler Gateway.
2. Las directivas de autenticación avanzada no están vinculadas al servidor virtual de autenticación y el mismo servidor virtual de autenticación se menciona en `authnProfile`.
3. La cadena User-Agent de la solicitud HTTP coincide con los agentes de usuario configurados en `patset` ns_vpn_client_useragents.

Si no se cumplen estas condiciones, se utiliza la directiva de autenticación clásica vinculada a Gateway.

Si un agente de usuario, o parte de él, está vinculado a lo mencionado anteriormente `patset`, las solicitudes procedentes de esos agentes de usuario no participan en el flujo de nFactor. Por ejemplo, el siguiente comando restringe la configuración de todos los exploradores (suponiendo que todos los exploradores contengan "Mozilla"en la cadena user-agent):

```
bind patset ns_vpn_client_useragents Mozilla
<!--NeedCopy-->
```

LoginSchema

LoginSchema es una representación lógica del formulario de inicio de sesión. El lenguaje XML lo define. La sintaxis de LoginSchema se ajusta a la especificación Common Forms Protocol de Citrix.

LoginSchema define la "vista"del producto. Un administrador puede proporcionar una descripción personalizada, texto de ayuda, etc. del formulario. El esquema de inicio de sesión incluye las etiquetas del propio formulario. Un cliente puede proporcionar el mensaje de éxito o fracaso que describe el formulario presentado en un momento determinado.

Utilice el siguiente comando para configurar un esquema de inicio de sesión.

```
add authentication loginSchema <name> -authenticationSchema <string> [-
    userExpression <string>] [-passwdExpression <string>] [-
    userCredentialIndex <positive_integer>]
[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
    <positive_integer>] [-SSOCredentials ( YES | NO )]
<!--NeedCopy-->
```

Descripción del parámetro

- name: nombre del nuevo esquema de inicio de sesión. Se trata de un argumento obligatorio. Longitud máxima: 127
- authenticationSchema: Nombre del archivo para leer el esquema de autenticación que se va a enviar para la interfaz de usuario de la página de inicio de sesión. Este archivo contiene la definición xml de los elementos según el Protocolo de autenticación de formularios de Citrix

para poder representar el formulario de inicio de sesión. Si el administrador no quiere solicitar otras credenciales a los usuarios, pero continúa con las credenciales obtenidas anteriormente, se puede dar `noschema` como argumento. Esto solo se aplica a los esquemas de inicio de sesión que se utilizan con los factores definidos por el usuario y no con el factor de servidor virtual.

Se trata de un argumento obligatorio. Longitud máxima: 255

- userExpression: Expresión para extraer el nombre de usuario durante el inicio de sesión. Esta puede ser cualquier expresión directiva avanzada relevante. Longitud máxima: 127
- passwdExpression: Expresión para extraer contraseñas durante el inicio de sesión. Esta puede ser cualquier expresión directiva avanzada relevante. Longitud máxima: 127
- userCredentialIndex: Índice en el que el usuario ha introducido el nombre de usuario debe almacenarse en la sesión. Valor mínimo: 1, Valor máximo: 16
- passwordCredentialIndex: El índice en el que el usuario ha introducido la contraseña debe almacenarse en la sesión. Valor mínimo: 1, Valor máximo: 16
- authenticationStrength: Peso de la autenticación actual Valor mínimo: 0, Valor máximo: 65535
- `SSOCredentials`: Esta opción indica si las credenciales de factor actuales son las credenciales de SSO (SingleSignOn) predeterminadas. Valores posibles: SÍ, NO. Valor por defecto: NO

Se requieren conocimientos de loginSchema y nFactor

Los archivos loginSchema precompilados se encuentran en la siguiente ubicación de NetScaler **/nsconfig/loginschema/LoginSchema/**. Estos archivos de loginSchema prediseñados se adaptan a casos de uso comunes y se pueden modificar para obtener ligeras variaciones si es necesario.

Además, la mayoría de los casos de uso de factor único con pocas personalizaciones no necesitan la configuración del esquema de inicio de sesión.

Se recomienda al administrador que consulte la documentación para ver otras opciones de configuración que permitan a NetScaler descubrir los factores. Una vez que el usuario envía las credenciales, el administrador puede configurar más de un factor para elegir y procesar de forma flexible los factores de autenticación.

Configuración de la autenticación de doble factor sin usar LoginSchema

NetScaler determina automáticamente los requisitos de doble factor según la configuración. Una vez que el usuario presenta estas credenciales, el administrador puede configurar el primer conjunto de directivas en el servidor virtual. En cada directiva, puede haber un "nextFactor"configurado como

un “passthrough”. Un “acceso directo”implica que NetScaler debe procesar el inicio de sesión con el conjunto de credenciales existente sin ir al usuario. Mediante el uso de factores de “acceso directo” , un administrador puede dirigir el flujo de autenticación mediante programación. Se recomienda a los administradores que lean la especificación nFactor o las guías de implementación para obtener más detalles. Consulte
Autenticación multifactor (nFactor).

Expresiones de nombre de usuario y contraseña

Para procesar las credenciales de inicio de sesión, el administrador debe configurar LoginSchema. Los casos de uso de factor único o doble factor con pocas personalizaciones de LoginSchema no necesitan una definición XML específica. LoginSchema tiene otras propiedades, como userExpression y passwdExpression, que se pueden utilizar para modificar el nombre de usuario o la contraseña que presenta el usuario.

Los esquemas de inicio de sesión son expresiones de directivas avanzadas y también se pueden utilizar para anular la entrada del usuario. Esto se puede lograr agregando una cadena para los parámetros en **-authenticationSchema**, como se muestra en el siguiente ejemplo.

A continuación se presentan los ejemplos para modificar las entradas de usuario para el nombre de usuario y la contraseña, respectivamente.

- Cambiar la entrada de usuario para el nombre de usuario de `username@citrix.com` a `username@xyz.com`

```
1 add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -userExpression "AAA.LOGIN.USERNAME.
    BEFORE_STR("@").APPEND("@xyz.com")"
2 <!--NeedCopy-->
```

- Considere un caso en el que el usuario proporciona una contraseña y un código de acceso en el primer factor como parte del esquema de inicio de sesión configurado. Para utilizar el **código** de acceso proporcionado por el usuario en el primer factor y la **contraseña** en el segundo factor, puede modificar el esquema de inicio de sesión existente mediante los siguientes comandos.

```
1 add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.
    PASSWORD2"
2 <!--NeedCopy-->
```

```
1 add authentication loginSchema user_schema_second -
    authenticationSchema noschema  -passwdExpression "AAA.LOGIN.
    PASSWORD"
2 <!--NeedCopy-->
```


Pasos de alto nivel en la configuración de n

El siguiente diagrama ilustra los pasos de alto nivel implicados en la configuración de nFactor.

Configuración GUI

En esta sección se describen los temas siguientes:

- Creación de un servidor virtual
- Crear servidor virtual de autenticación
- Crear perfil CERT de autenticación
- Creación de una directiva de autenticación
- Agregar un servidor de autenticación LDAP
- Agregar una directiva de autenticación LDAP
- Agregar un servidor de autenticación RADIUS
- Agregar una directiva de autenticación RADIUS
- Crear un esquema de inicio de sesión de autenticación
- Creación de una etiqueta de directiva

Crear un servidor virtual

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. Haga clic en el botón **Agregar** para crear un servidor virtual de puerta de enlace.
3. Introduzca la siguiente información y haga clic en **Aceptar**.

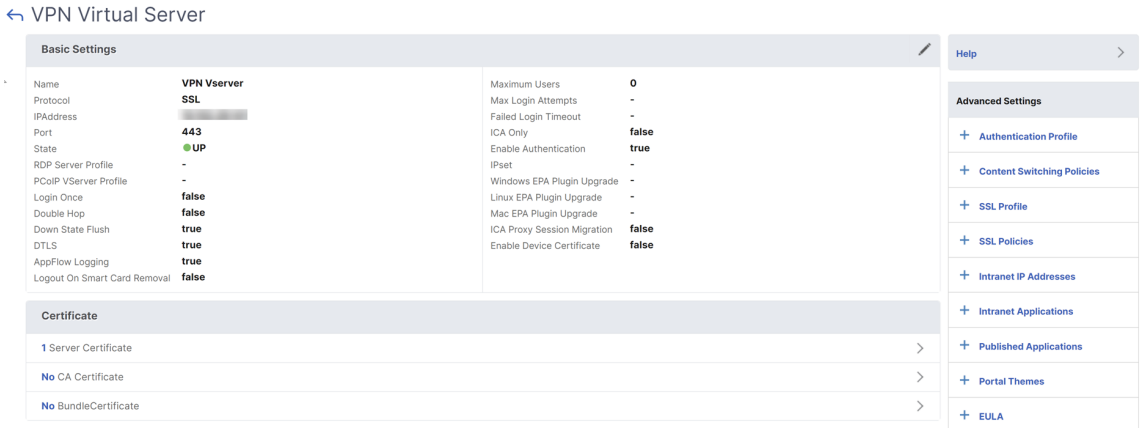
Nombre del parámetro	Descripción del parámetro
Escriba el nombre del servidor virtual.	Nombre del servidor virtual de NetScaler Gateway. Debe comenzar con un carácter alfabético ASCII o de subrayado (_) y debe contener solo caracteres alfanuméricos ASCII, guión bajo, hash (#), punto (.), espacio, dos puntos (:), en (@), igual (=) y guión (-). Se puede cambiar una vez creado el servidor virtual. El siguiente requisito solo se aplica a la CLI de NetScaler: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, “mi servidor”o “mi servidor”).
Introduzca el tipo de dirección IP del servidor virtual	Seleccione una opción Dirección IP o No direccionable del menú desplegable.
Introduzca la dirección IP del servidor virtual.	Una dirección de protocolo de Internet (dirección IP) es una etiqueta numérica asignada a cada dispositivo que participa en la red informática que utiliza el protocolo de Internet para la comunicación.
Introduzca el número de puerto del servidor virtual.	Introduzca el número de puerto.
Introduzca el perfil de autenticación.	Entidad de perfil de autenticación en el servidor virtual. Esta entidad se puede utilizar para descargar la autenticación al servidor virtual de autenticación, autorización y auditoría para la autenticación multifactor (nFactor)
Introduzca el perfil del servidor RDP.	Nombre del perfil del servidor RDP asociado al servidor virtual.

Nombre del parámetro	Descripción del parámetro
Introduzca el número máximo de usuarios.	Número máximo de sesiones de usuario simultáneas permitidas en este servidor virtual. El número real de usuarios permitidos para iniciar sesión en este servidor virtual depende del número total de licencias de usuario.
Introduzca el número máximo de intentos de inicio	Número máximo de intentos de inicio de sesión.
Escriba el tiempo de espera de inicio de sesión fallido.	Número de minutos que se bloquea una cuenta si el usuario supera el número máximo de intentos permitidos.
Introduzca a la actualización del plug-in de EPA de Windows.	Opción para establecer el comportamiento de actualización de plug-ins para Win.
Introduzca la actualización del complemento EPA de Linux.	Opción para establecer el comportamiento de actualización de plug-ins para Linux.
Introduzca la actualización del plug-in MAC EPA	Opción para establecer el comportamiento de actualización de plug-ins para Mac.
Login Once	Esta opción habilita o inhabilita el SSO sin interrupciones para este servidor virtual.

Nombre del parámetro	Descripción del parámetro
Solo ICA	Cuando se establece en ON, implica el modo Básico, en el que el usuario puede iniciar sesión con la aplicación Citrix Workspace o con un explorador y obtener acceso a las aplicaciones publicadas configuradas en el entorno de Citrix Virtual Apps and Desktops señalado por el parámetro `Wihome`. Los usuarios no pueden conectarse mediante el cliente Citrix Secure Access y no se pueden configurar los escaneos de puntos finales. El número de usuarios que pueden iniciar sesión y acceder a las aplicaciones no está limitado por la licencia de este modo. - Cuando se establece en OFF, implica el modo SmartAccess, en el que el usuario puede iniciar sesión mediante la aplicación Citrix Workspace, un explorador web o un cliente Citrix Secure Access. El administrador puede configurar los análisis de puntos finales para que se ejecuten en los sistemas cliente y, a continuación, utilizar los resultados para controlar el acceso a las aplicaciones publicadas. En este modo, el cliente puede conectarse a la puerta de enlace en otros modos de cliente, como VPN y VPN sin cliente. El número de usuarios que pueden iniciar sesión y acceder a los recursos está limitado por las licencias de la CCU en este modo.
Habilitar autenticación	Requiere autenticación para los usuarios que se conectan a NetScaler Gateway.

Nombre del parámetro	Descripción del parámetro
Doble salto	Utilice el dispositivo NetScaler Gateway en una configuración de doble salto. Una implementación de doble salto proporciona una capa adicional de seguridad para la red interna mediante el uso de tres firewalls para dividir la DMZ en dos etapas. Dicha implementación puede tener un dispositivo en la DMZ y un dispositivo en la red segura.
Flush de estado descendente	Cierre las conexiones existentes cuando el servidor virtual esté marcado como DOWN, lo que significa que es posible que el servidor haya agotado el tiempo de espera. La desconexión de las conexiones existentes libera recursos y, en algunos casos, acelera la recuperación de configuraciones de equilibrio de carga sobrecargadas. Habilite este ajuste en los servidores en los que las conexiones se puedan cerrar de forma segura cuando estén marcadas como DOWN. No habilite el vaciado de estado DOWN en los servidores que deben completar sus transacciones.
DTLS	Esta opción inicie/detiene el servicio de turno en el servidor virtual
Registro de AppFlow	Registre registros de AppFlow que contienen información estándar de NetFlow o IPFIX, como marcas de tiempo para el inicio y el final de un flujo, recuento de paquetes y recuento de bytes. También registra registros que contienen información a nivel de aplicación, como direcciones web HTTP, métodos de solicitud HTTP y códigos de estado de respuesta, tiempo de respuesta del servidor y latencia.
Migración de sesión proxy ICA	Esta opción determina si se transfiere una sesión de proxy ICA existente cuando el usuario inicie sesión desde otro dispositivo.
State	El estado actual del servidor virtual, como UP, DOWN, BUSY, etc.

Nombre del parámetro	Descripción del parámetro
Habilitar certificado de dispositivo	Indica si la comprobación del certificado de dispositivo como parte de EPA está activada o desactivada.



4. Seleccione la sección **Sin certificado de servidor** de la página.
5. Haga clic en ****en **Seleccionar certificado de servidor** para seleccionar el certificado de servidor.
6. Seleccione el Certificado SSL y haga clic en el botón **Seleccionar**.
7. Haga clic en **Bind**.
8. Si aparece una advertencia sobre **No hay cifrados utilizables**, haga clic en **Aceptar**
9. Haga clic en el botón **Continuar**.
10. En la sección Autenticación, haga clic en el icono **+** en la parte superior derecha.

Creación de un servidor virtual de autenticación

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Servidores virtuales.**
2. Haga clic en el botón **Add**.
3. Complete la siguiente configuración básica para crear el servidor virtual de autenticación.

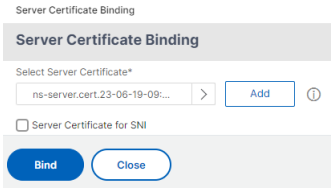
   Nota: El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   - Introduzca el **nombre** del nuevo servidor virtual de autenticación.
   - Introduzca el **tipo de dirección IP**. El tipo de dirección IP se puede configurar como no direccionable.

- Introduzca la **dirección IP**. La dirección IP puede ser cero.
- Introduzca el tipo de **protocolo** del servidor virtual de autenticación.
- Introduzca el **puerto TCP** en el que el servidor virtual acepta conexiones.
- Introduzca el **dominio** de la cookie de autenticación establecida por el servidor virtual de autenticación.

4. Haga clic en **Aceptar**.
5. Haga clic en la sección **Sin certificado de servidor** .
6. Haga clic en ** en **Seleccionar certificado de servidor**.
7. Elija el certificado SSL deseado y haga clic en el botón **Seleccionar**.

   Nota: El servidor virtual de autenticación no necesita un certificado vinculado a él.
8. Configure el **enlace de certificados de servidor**.
   - Marque la casilla **Certificado de servidor para SNI** para enlazar una o más claves de certificado utilizadas para el procesamiento de SNI.
   - Haga clic en el botón **Vincular**.



Crear un perfil CERT de autenticación

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Directivas > Autenticación > Directivas básicas > CERT.**
2. Seleccione la ficha Perfiles y, a continuación, seleccione **Agregar**.
3. Complete los campos siguientes para crear el perfil CERT de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.
   - **Nombre**: Nombre del perfil del servidor de autenticación del certificado del cliente (acción).
   - **Dos factores**: En este caso, la opción de autenticación de dos factores es NOOP.
   - **Campo Nombre de usuario**: Introduzca el campo client-cert del que se extrae el nombre de usuario. Debe establecerse en “Asunto”o “Emisor”(incluir ambos juegos de comillas dobles).

- **Campo de nombre de grupo**: Introduzca el campo cliente-cert del que se extrae el grupo. Debe establecerse en "Asunto"o "Emisor"(incluir ambos juegos de comillas dobles).
- **Grupo de autenticación predeterminado**: Es el grupo predeterminado que se elige cuando la autenticación se realiza correctamente además de los grupos extraídos.

4. Haga clic en **Crear**.

Crear una directiva de autenticación

> **Nota**
>
> Si configura una directiva de primer factor con una regla de directivas mediante AAA.login, la siguiente expresión debe configurarse con la condición OR para que la aplicación Citrix Workspace admita la implementación de nFactor.
>
> ```
> || HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
> ```

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directiva.**
2. Seleccione el botón **Agregar**
3. Complete la siguiente información para crear una directiva de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   a) **Nombre**: Introduzca el nombre de la directiva de autenticación avanzada. Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la directiva de autenticación.

   El siguiente requisito solo se aplica a la CLI de NetScaler: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "mi directiva de autenticación"o "mi directiva de autenticación").

   b) **Tipo de acción**: Introduzca el tipo de acción de autenticación.

   c) **Acción**: Introduzca el nombre de la acción de autenticación que se realizará si la directiva coincide.

   d) **Acción de registro**: Introduzca el nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

   e) **Expresión**: Introduzca el nombre de la regla con nombre de NetScaler, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se intenta autenticar al usuario con el servidor AUTHENTICATION.

   f) **Comentarios**: Introduzca cualquier comentario para conservar la información sobre esta directiva.

4. Haga clic en **Crear**.

Agregar un servidor de autenticación LDAP

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Directivas > Autenticación > Directivas básicas > LDAP**.
2. Agregue un servidor LDAP seleccionando la ficha **Servidor** y seleccionando el botón **Agregar**.

Agregar una directiva de autenticación LDAP

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directiva**.
2. Haga clic en **Agregar** para agregar una directiva de autenticación.
3. Complete la siguiente información para crear una directiva de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.

   a) **Nombre: nombre** de la directiva AUTENTICACIÓN avanzada.
   Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la directiva de autenticación.

   El siguiente requisito solo se aplica a la CLI de NetScaler: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "mi directiva de autenticación"o "mi directiva de autenticación").

   b) **Tipo de acción**: Tipo de acción de autenticación.

   c) **Acción**: Nombre de la acción de autenticación que se va a realizar si la directiva coincide.

   d) **Acción de registro**: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

   e) **Expresión**: Nombre de la regla con nombre de NetScaler, o una expresión de sintaxis predeterminada, que la directiva utiliza para determinar si se intenta autenticar al usuario con el servidor AUTHENTICATION.

   f) **Comentarios**: Cualquier comentario para preservar la información sobre esta directiva.
4. Haga clic en **Crear.**

Agregar un servidor de autenticación RADIUS

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Autenticación de directivas > Directivas básicas > RADIUS**.

2. Para agregar un servidor, seleccione la ficha **Servidores** y seleccione el botón **Agregar**.
3. Introduzca lo siguiente para crear un servidor RADIUS de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.
    a) Escriba un **nombre** para la acción RADIUS.
    b) Introduzca el **nombre del servidoro la dirección IP del servidor** asignados al servidor RADIUS.
    c) Introduzca el número de **puerto** en el que el servidor RADIUS escucha las conexiones.
    d) Introduzca el valor Tiempo de **espera** en unos segundos. El dispositivo NetScaler espera una respuesta del servidor RADIUS hasta que caduque el valor de tiempo de espera configurado.
    e) Introduzca la **clave secreta** compartida entre el servidor RADIUS y el dispositivo NetScaler. La clave secreta es necesaria para permitir que el dispositivo NetScaler se comunique con el servidor RADIUS.
    f) **Confirma la clave secreta**.
4. Haga clic en **Crear.**

Agregar una directiva de autenticación RADIUS

1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directiva.**
2. Haga clic en **Agregar** para crear una directiva de autenticación.
3. Complete la siguiente información para crear una directiva de autenticación. El signo * situado a la derecha del nombre de la configuración indica campos obligatorios.
    a) **Nombre**: Nombre de la directiva AUTHENTICATION avanzada.
    Debe comenzar con una letra, un número o un carácter de guión bajo (_) y debe contener solo letras, números y guión (-), punto (.) almohadilla (#), espacio (), en (@), igual a (=), dos puntos (:) y guión bajo. No se puede cambiar una vez creada la directiva AUTENTICACIÓN.

    El siguiente requisito solo se aplica a la CLI de NetScaler: Si el nombre incluye uno o más espacios, escriba el nombre entre comillas dobles o simples (por ejemplo, "mi directiva de autenticación"o "mi directiva de autenticación").

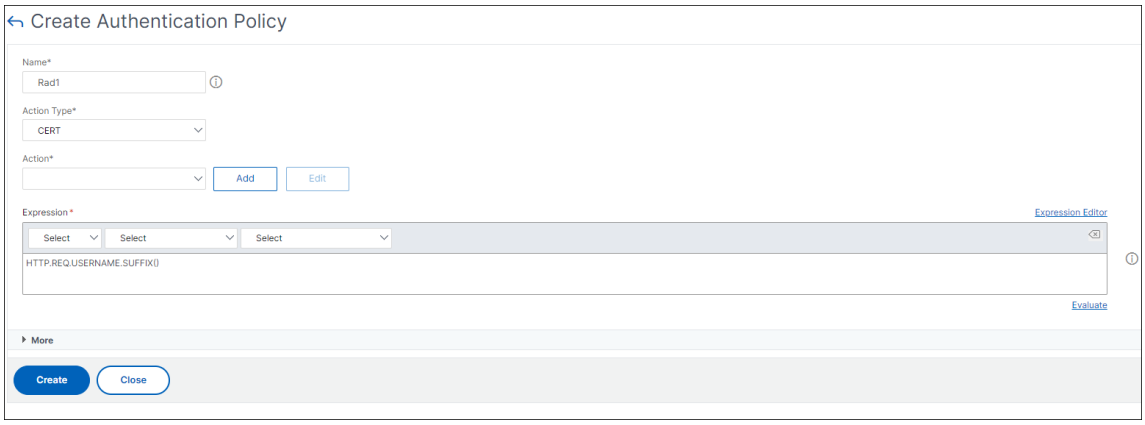
    a) **Tipo de acción**: Tipo de acción de autenticación.
    b) **Acción**: Nombre de la acción de autenticación que se va a realizar si la directiva coincide.

c) **Acción de registro**: Nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva.

d) **Expresión**: Nombre de la regla denominada de NetScaler o expresión de sintaxis predeterminada que utiliza la directiva para determinar si se intenta autenticar al usuario en el servidor AUTHENTICATION.

e) **Comentarios**: Cualquier comentario para preservar la información sobre esta directiva.

4. Haga clic en **Aceptar.** La directiva de autenticación que creó aparece en la lista de directivas.



Crear un esquema de inicio de sesión de autenticación

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Esquema de inicio de sesión.**
2. Seleccione la ficha Perfiles y haga clic en el botón **Agregar**.
3. Complete los campos siguientes para crear un esquema de inicio de sesión de autenticación:

   a) Introducir **nombre**: Nombre para el nuevo esquema de inicio de sesión.

   b) Introducir **esquema de autenticación**: Nombre del archivo para leer el esquema de autenticación que se va a enviar para la interfaz de usuario de la página de inicio de sesión. Este archivo debe contener la definición xml de los elementos según el Protocolo de autenticación de Citrix Forms para poder generar un formulario de inicio de sesión. Si un administrador no quiere solicitar más credenciales a los usuarios, pero continúa con las credenciales obtenidas anteriormente, se puede darnoschema"""como argumento. Esto solo se aplica a los loginSchemas que se utilizan con factores definidos por el usuario y no al factor de servidor virtual

   c) Introducir **expresión de usuario**: Expresión para extraer el nombre de usuario durante el inicio de sesión

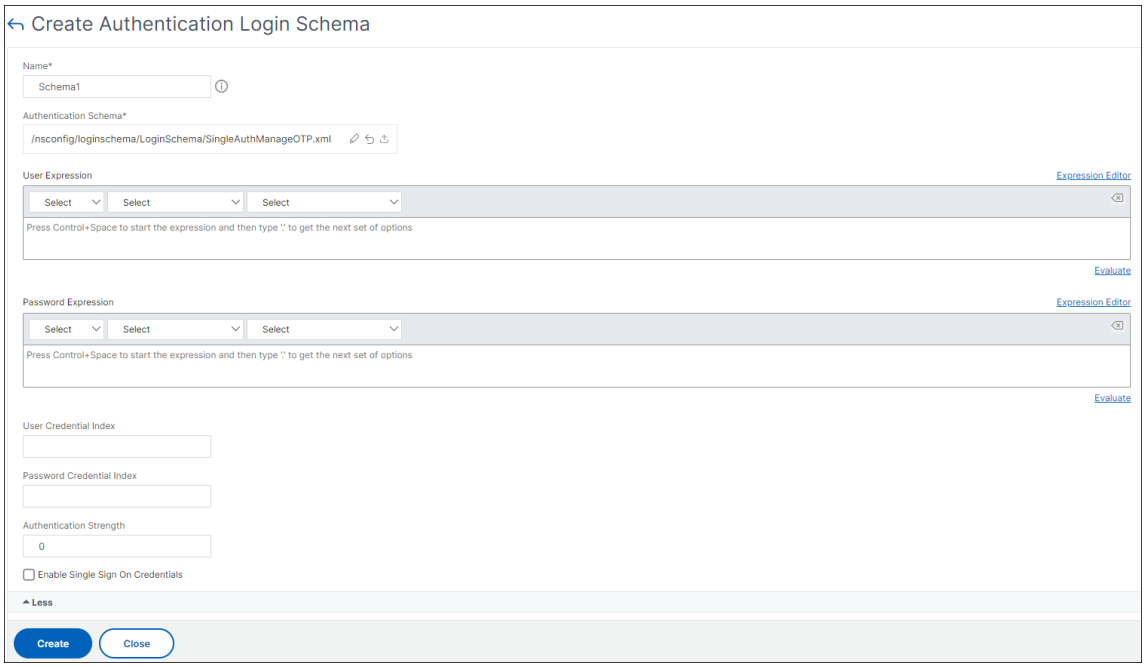
   d) Introducir **expresión de contraseña**: Expresión para extraer la contraseña durante el inicio de sesión

e) Introducir **índice de credenciales de usuario**: Índice en el que el nombre de usuario introducido por el usuario se almacena en la sesión.

f) Introducir **índice de credenciales de contraseña:** Índice en el que el usuario ha introducido la contraseña debe almacenarse en la sesión.

g) Introduzca **Fuerza de autenticación**: Peso de la autenticación actual.

4. Haga clic en **Crear.** El perfil de esquema de inicio de sesión que creó debe aparecer en la lista de perfiles de esquema de inicio de sesión.



Crear una etiqueta de directiva

Una etiqueta de directiva especifica las directivas de autenticación de un factor concreto. Cada etiqueta de directiva corresponde a un único factor. La etiqueta de directiva especifica el formulario de inicio de sesión que debe presentarse al usuario. La etiqueta de directiva debe estar vinculada como el siguiente factor de una directiva de autenticación o de otra etiqueta de directiva de autenticación. Normalmente, una etiqueta de directiva incluye directivas de autenticación para un mecanismo de autenticación específico. Sin embargo, también puede tener una etiqueta de directiva que tenga directivas de autenticación para distintos mecanismos de autenticación.

1. Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Políticas > Autenticación > Políticas avanzadas > Etiqueta de política.**
2. Haga clic en el botón **Add**.
3. Complete los campos siguientes para crear una etiqueta de directiva de autenticación:

a) Introduzca el **nombre** de la nueva etiqueta de directiva de autenticación.

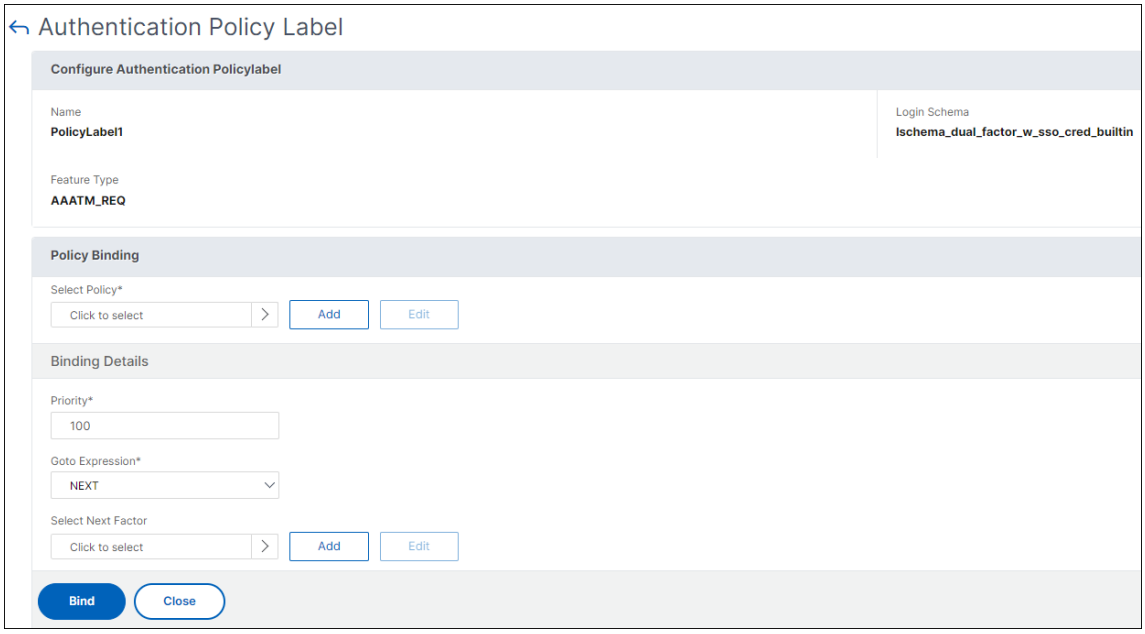
b) Introduzca el **esquema de inicio** de sesión asociado a la etiqueta de directiva de autenticación.

c) Haga clic en **Continuar**.

4. **Seleccione una directiva** en el menú desplegable.
5. Elija la **directiva de autenticación** deseada y haga clic en el botón **Seleccionar**.
6. Rellene los campos siguientes:

a) Introduzca la **prioridad** de la vinculación de la directiva.

b) Introduzca la **expresión Goto**: La expresión especifica la prioridad de la siguiente directiva que se evaluará si la regla de directiva actual se evalúa como TRUE.



7. Seleccione la directiva de autenticación deseada y haga clic en el botón **Seleccionar**.
8. Haga clic en el botón **Vincular**.
9. Haga clic en **Listo**.
10. Revise la etiqueta de directiva de autenticación.

Configuración re-Captcha para autenticación nFactor

A partir de la versión 12.1 compilación 50.x de NetScaler, NetScaler Gateway admite una nueva acción de primera clase "captchaAction"que simplifica la configuración de Captcha. Como Captcha es una

acción de primera clase, puede ser un factor propio. Puede inyectar Captcha en cualquier parte del flujo de nFactor.

Anteriormente, tenías que escribir directivas WebAuth personalizadas con cambios en la RfWebUI también. Con la introducción de captchaAction, no es necesario modificar el JavaScript.

> **Importante**
>
> Si se utiliza Captcha junto con campos de nombre de usuario o contraseña en el esquema, el botón Enviar se desactiva hasta que se cumpla el Captcha.

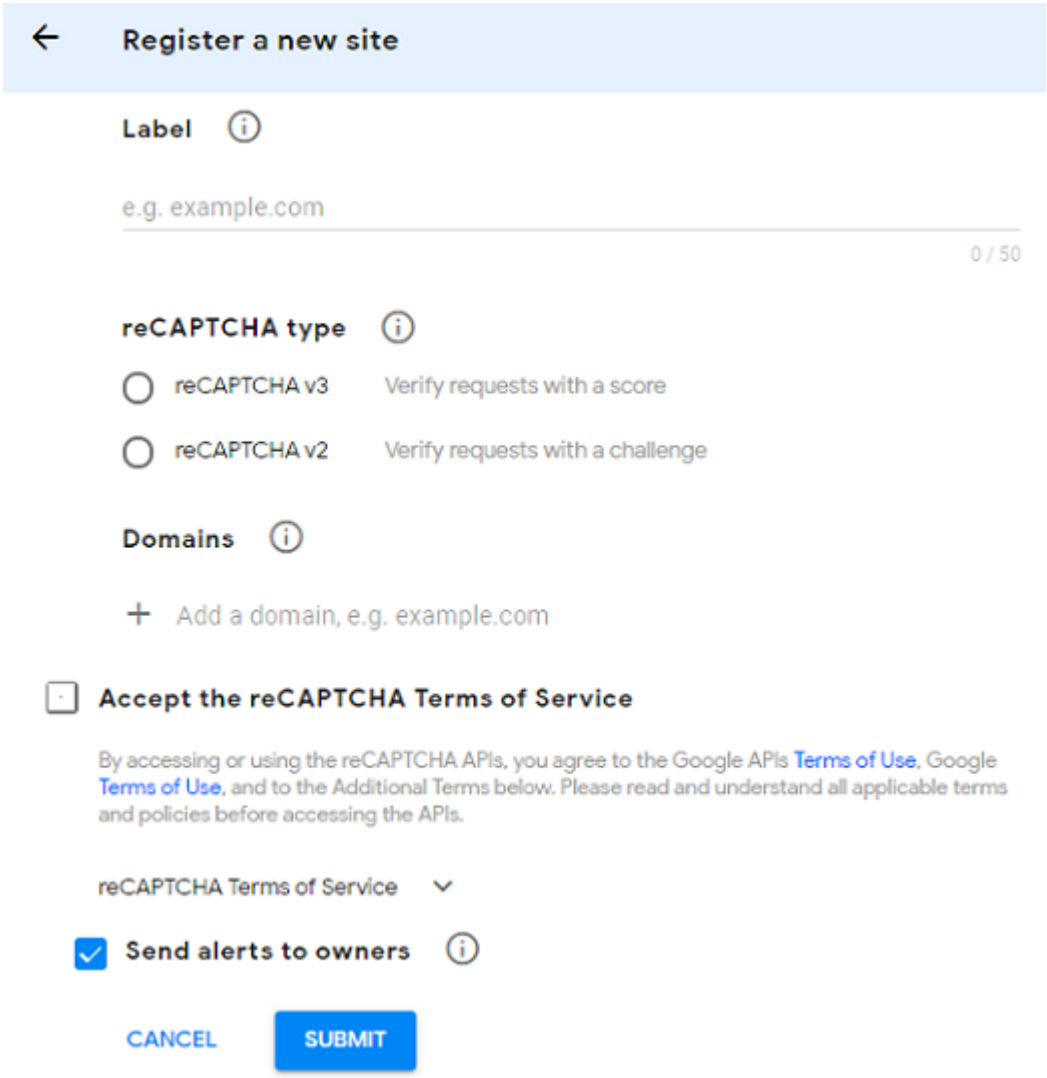
Configuración de captcha

La configuración de captcha consta de dos partes.

1. Configuración en Google para registrar Captcha.
2. Configuración en el dispositivo NetScaler para utilizar Captcha como parte del flujo de inicio de sesión.

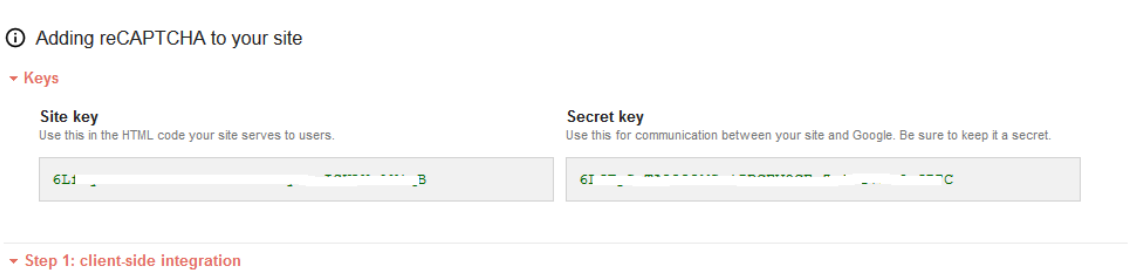
Configuración de captcha en Google Registre un dominio para Captcha en `https://www.google.com/recaptcha/admin#list`.

1. Al navegar a esta página, aparece la siguiente pantalla.



> **Nota**
>
> Utilice únicamente la versión 2 de `reCAPTCHA`. El `reCAPTCHA` invisible sigue en vista previa.

2. Después de registrar un dominio, se muestran "SiteKey"y "SecretKey".



> **Nota**
>
> La "SiteKey"y la "SecretKey"están atenuadas por motivos de seguridad. "SecretKey"debe mantenerse a salvo.

Configuración de captcha en el dispositivo NetScaler La configuración de Captcha en el dispositivo NetScaler se puede dividir en tres partes:

- Mostrar pantalla Captcha
- Publicar la respuesta Captcha en el servidor de Google
- La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional)

Mostrar pantalla Captcha La personalización del formulario de inicio de sesión se realiza mediante el esquema de inicio de sesión SingleAuthCaptcha.xml. Esta personalización se especifica en el servidor virtual de autenticación y se envía a la interfaz de usuario para representar el formulario de inicio de sesión. El esquema de inicio de sesión integrado, SingleAuthCaptcha.xml, se encuentra en el directorio /nsconfig/loginSchema/LoginSchema del dispositivo NetScaler.

> **Importante**
>
> - En función de su caso de uso y de los diferentes esquemas, puede modificar el esquema existente. Por ejemplo, si solo necesitas factor Captcha (sin nombre de usuario ni contraseña) o autenticación dual con Captcha.
> - Si se realizan modificaciones personalizadas o se cambia el nombre del archivo, Citrix recomienda copiar todos los esquemas de inicio de sesión del directorio /nsconfig/loginschema/loginSchema en el directorio principal, /nsconfig/loginschema.

Para configurar la visualización de Captcha mediante CLI

```
1 - add authentication loginSchema singleauthcaptcha -
    authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3 - add authentication loginSchemaPolicy singleauthcaptcha -rule true -
    action singleauthcaptcha
4
5 - add authentication vserver auth SSL <IP> <Port>
6
7 - add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to
    -key-file>
8 - bind ssl vserver auth -certkey vserver-cert
9 - bind authentication vserver auth -policy singleauthcaptcha -priority
     5 -gotoPriorityExpression END
10 <!--NeedCopy-->
```


Publicar la respuesta Captcha en el servidor de Google Una vez configurado el Captcha que debe mostrarse a los usuarios, los administradores publican la configuración en el servidor de Google para verificar la respuesta de Captcha desde el explorador.

Para verificar la respuesta de Captcha desde el explorador

```
1 - add authentication captchaAction myrecaptcha -sitekey <sitekey-
    copied-from-google> -secretkey <secretkey-from-google>
2
3 - add authentication policy myrecaptcha -rule true -action myrecaptcha
4 - bind authentication vserver auth -policy myrecaptcha -priority 1
5 <!--NeedCopy-->
```

Los siguientes comandos son necesarios para configurar si se quiere la autenticación de AD. De lo contrario, puede ignorar este paso.

```
1 - add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
     636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn
    adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -
    encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
     memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -
    defaultAuthenticationGroup ldapGroup
2
3 - add authenticationpolicy ldap-new -rule true -action ldap-new
4 <!--NeedCopy-->
```

La configuración LDAP es el segundo factor para el inicio de sesión del usuario (opcional) La autenticación LDAP se produce después de Captcha, se agrega al segundo factor.

```
1 - add authentication policylabel second-factor
2 - bind authentication policylabel second-factor -policy ldap-new -
    priority 10
3 - bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
4 <!--NeedCopy-->
```

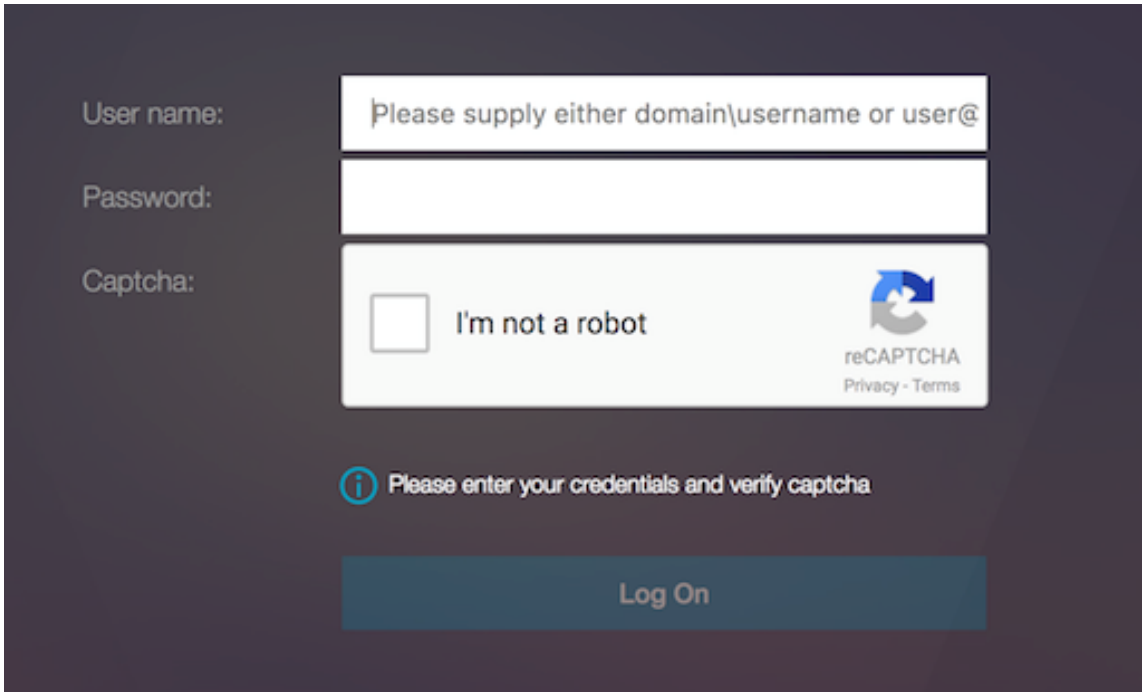
El administrador debe agregar los servidores virtuales adecuados en función de si se utiliza un servidor virtual de equilibrio de carga o un dispositivo NetScaler Gateway para el acceso. El administrador debe configurar el siguiente comando si se necesita un servidor virtual de equilibrio de carga:

```
1 add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com`
2 <!--NeedCopy-->
```

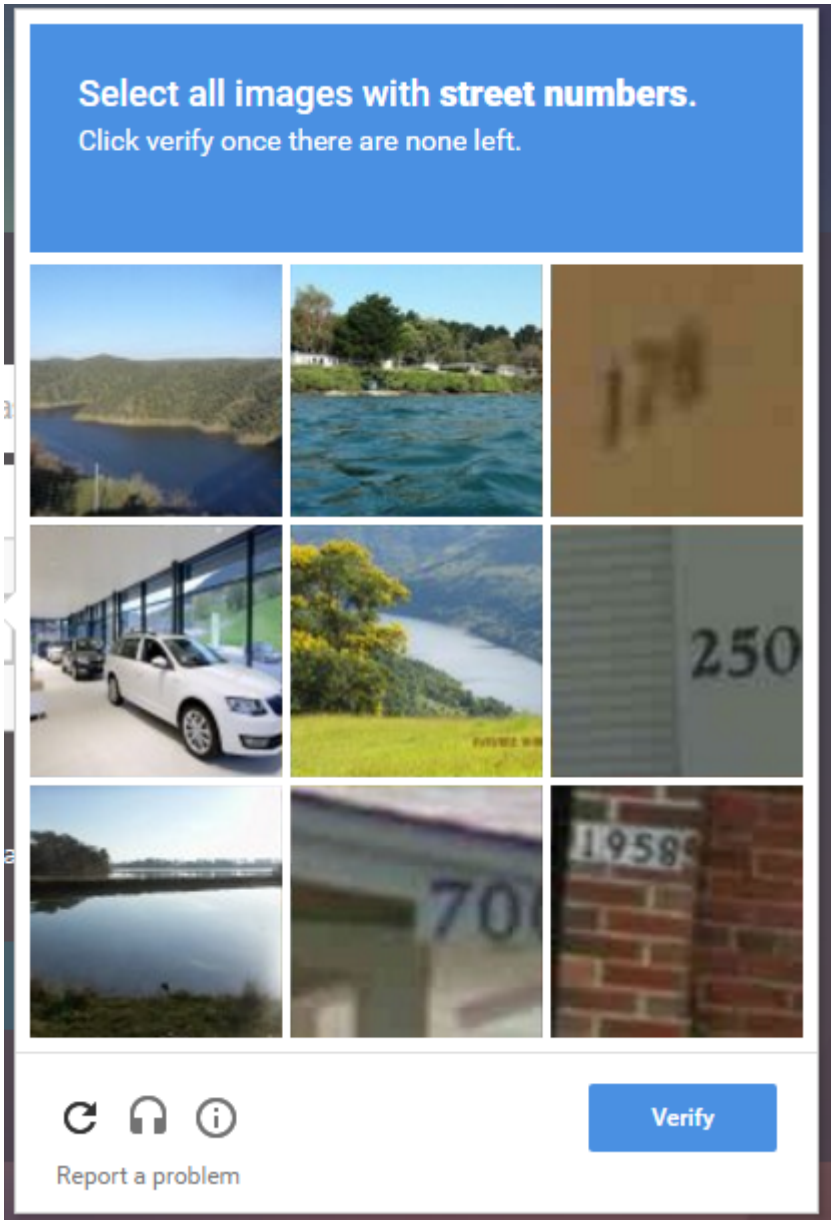
nssp.aaatm.com: Se resuelve en el servidor virtual de autenticación.

Validación de usuario de Captcha Una vez configurados todos los pasos mencionados en las secciones anteriores, consulte las capturas de pantalla anteriores de la interfaz de usuario.

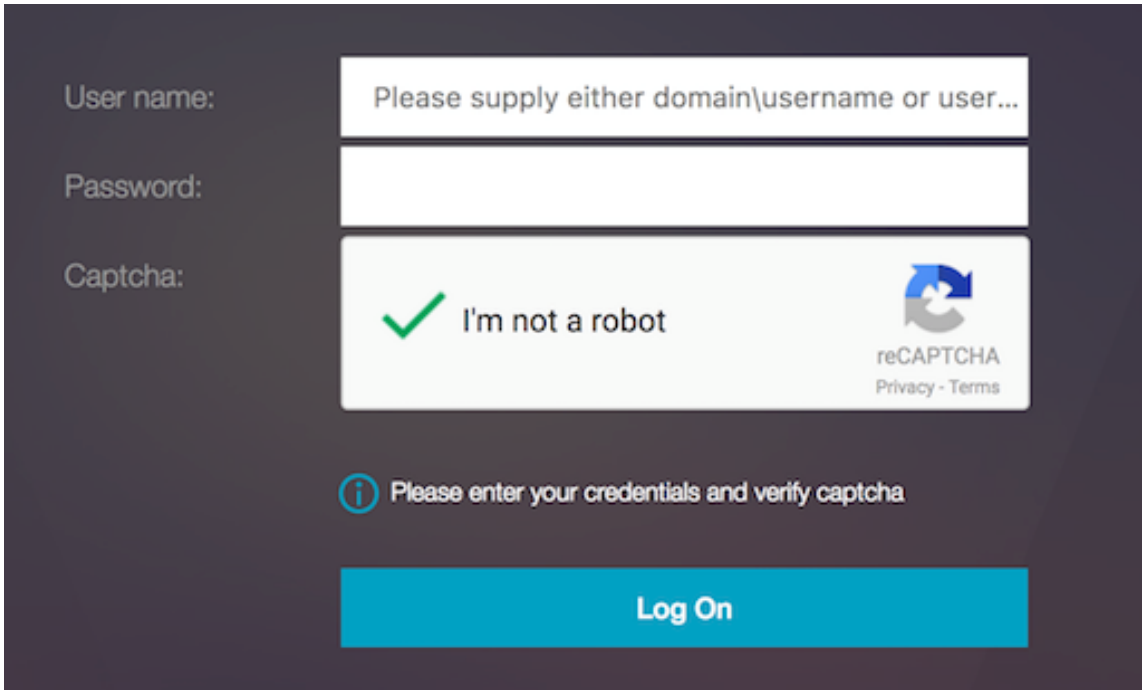
1. Una vez que el servidor virtual de autenticación carga la página de inicio de sesión, aparece la pantalla de inicio de sesión. El**inicio de sesión** está inhabilitado hasta que se complete Captcha.



2. Selecciona la opción No soy un robot. Se muestra el widget Captcha.



3. Se navega por una serie de imágenes Captcha antes de que se muestre la página de finalización.
4. Introduzca las credenciales de AD, active la casilla de verificación **No soy un robot** y haga clic **en Iniciar sesión**. Si la autenticación se realiza correctamente, se le redirigirá al recurso deseado.

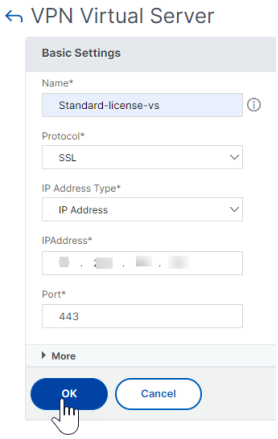


Nota:

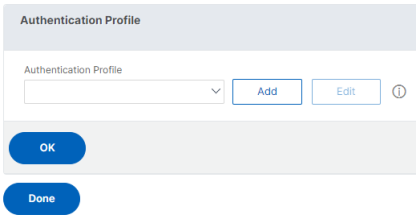
- Si se utiliza Captcha con autenticación de AD, el botón Enviar para las credenciales se inhabilita hasta que se complete Captcha.
- El Captcha ocurre en un factor propio. Por lo tanto, cualquier validación posterior como AD debe realizarse en `nextfactor` del Captcha.

Crear un servidor virtual de puerta de enlace para la autenticación nFactor en la licencia NetScaler Standard

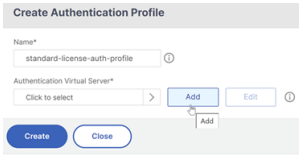
1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. En la página **Servidores virtuales de NetScaler Gateway**, haga clic en **Agregar**.
3. Introduzca los siguientes detalles en la página del **servidor virtual VPN**, haga clic en **Aceptar** y, a continuación, en **Continuar**.
    - Nombre: Nombre del servidor virtual de NetScaler Gateway
    - Protocolo: seleccione **SSL**
    - Dirección IP: dirección IP del servidor virtual NetScaler Gateway
    - Puerto: introduzca 443



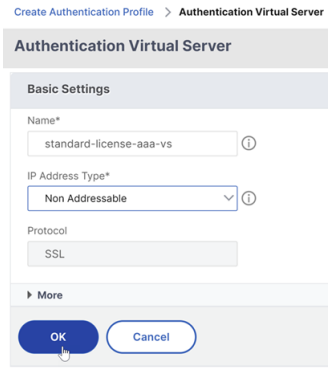
1. En la página **Servidor virtual de VPN**, haga clic en el icono más situado junto a **Perfil de autenticación**.
2. Haga clic en **Agregar** para configurar el perfil de autenticación.



3. Introduzca un nombre para el perfil de autenticación y haga clic en **Agregar**.



4. Introduzca los siguientes detalles en la página del **servidor virtual VPN** , haga clic en Aceptar **y,** a continuación, en **Continuar** .
   - Nombre: nombre del servidor virtual de autenticación, autorización y auditoría
   - Protocolo: seleccione **No direccionable**. Solo un servidor virtual de autenticación, autorización y auditoría no direccionable se puede vincular a un servidor virtual de puerta de enlace o VPN en la licencia NetScaler Standard.



Nota:

- En la licencia NetScaler Standard, los pasos para crear directivas son los mismos que los de la licencia Premium para los tipos de directivas compatibles.
- La licencia NetScaler Standard no admite la adición de nuevos esquemas de inicio de sesión en la configuración de nFactor.

Referencias

Para ver un ejemplo de configuración de nFactor de extremo a extremo, consulte Configuración de la autenticación de nFactor.

Visualizador de Unified Gateway

March 27, 2024

El visualizador de Unified Gateway proporciona una representación visual de las configuraciones mediante el Asistente de Unified Gateway. El visualizador de Unified Gateway se utiliza para agregar y modificar la configuración y diagnosticar un problema de back-end.

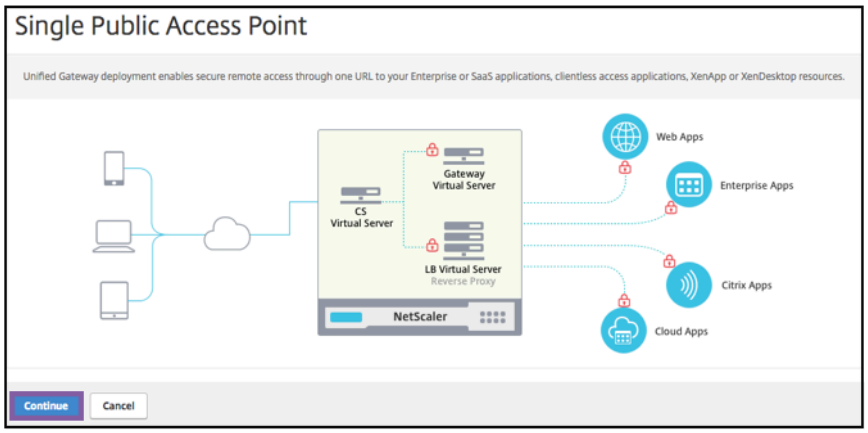
El visualizador de Unified Gateway muestra lo siguiente:

Configuración	Configuración
Directivas de autenticación previa	Directivas de autenticación
Servidores virtuales CS	Servidores virtuales VPN
Servidores virtuales LB	Aplicaciones XA/XD
Aplicaciones web	Aplicaciones SaaS

La implementación de Unified Gateway permite un acceso remoto seguro mediante una URL a sus aplicaciones empresariales o SaaS, aplicaciones de acceso sin cliente, recursos de Citrix Virtual Apps y Desktops.

Configurar Unified Gateway

1. Seleccione Unified Gateway en el menú.
2. En la siguiente pantalla, compruebe que dispone de la siguiente información y, a continuación, haga clic en **Comenzar**:
   - Dirección IP pública de Unified Gateway.
   - Cadena de certificados de servidor (.PFX o.PEM) con certificado Root-CA opcional.
   - Detalles de autenticación basada en LDAP/RADIUS/certificado de cliente.
   - Detalles de la aplicación (URL de aplicaciones SaaS o detalles del servidor Citrix Virtual Apps and Desktops).
3. Haga clic en el botón **Continuar**.



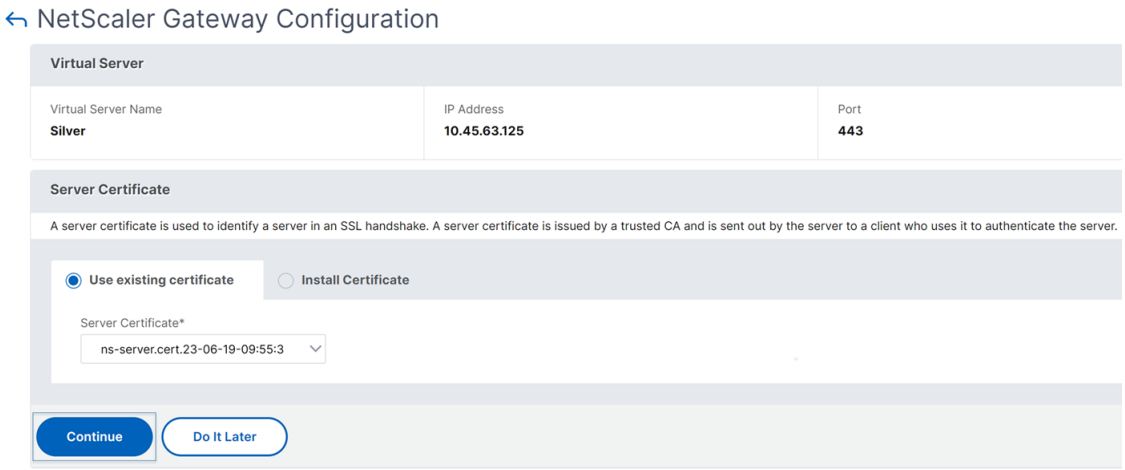
Cree un servidor virtual de configuración de Unified Gateway.

1. Introduzca el **nombre** de configuración del servidor virtual.
2. Introduzca la **dirección IP pública de Unified Gateway** para la implementación de Unified Gateway.
3. Introduzca el nombre de dominio completo (**FQDN**) para la implementación de Unified Gateway.
4. Introduzca el número de **puerto**. El intervalo de números de puerto es del 1 al 65535.
5. Haga clic en **Continuar**.

Complete la siguiente información para especificar el certificado de servidor.

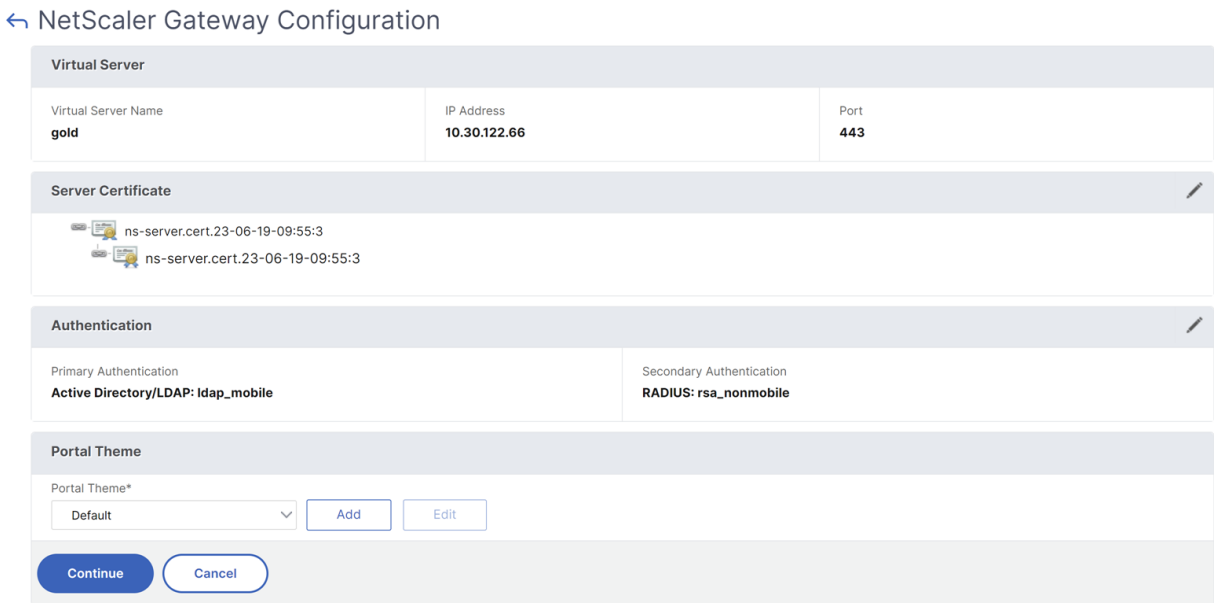
1. Seleccione los botones de opción **Usar certificado existente** o **Instalar certificado**.

2. Seleccione un **certificado de servidor** en el menú.
3. Haga clic en el botón **Continuar**.



Complete la siguiente información para especificar la autenticación.

1. Seleccione un **método de autenticación principal** en el menú.
2. Seleccione los botones de opción **Usar servidor existente** o **Agregar servidor nuevo** para especificar los detalles del servidor de autenticación principal.
3. Seleccione un **método de autenticación secundario** en el menú.
4. Seleccione los botones de opción **Usar servidor existente** o **Agregar servidor nuevo** para especificar los detalles del servidor de autenticación secundario.
5. Haga clic en el botón **Continuar**.
6. Selecciona el **tema del portal** en el menú.
7. Haga clic en **Continuar**.
8. Seleccione los botones de opción **Aplicación web** o **Escritorios de Citrix Virtual Apps**.
9. Haga clic en **Continuar**.



Seleccionar aplicación

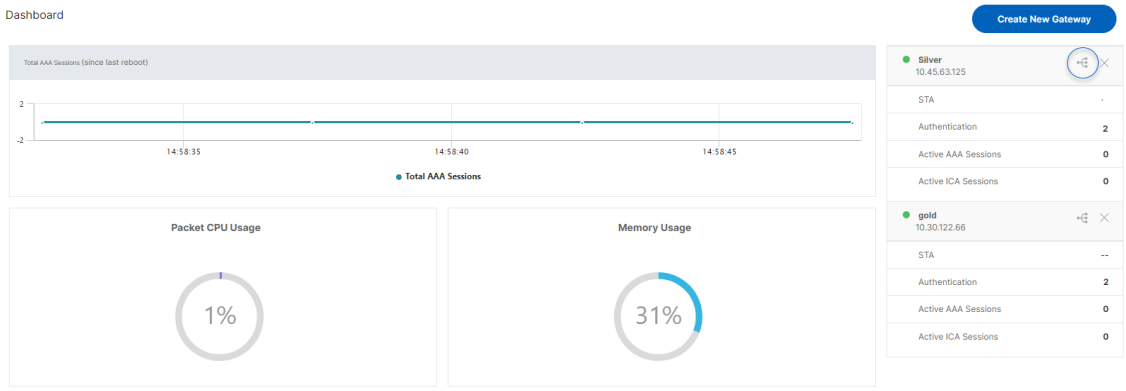
Complete la siguiente información para especificar la aplicación web.

1. Introduzca el nombre del enlace del marcador.
2. Seleccione el tipo de aplicación que representa la URL de VPN. Los valores posibles son:
   - Aplicación de intranet
   - Acceso sin cliente
   - SaaS
   - Aplicación preconfigurada en este NetScaler
3. Marque esta casilla para que esta aplicación sea accesible a través de la URL de Unified Gateway.
4. Introduzca la URL del enlace del marcador.
5. En la URL del icono, elige un archivo para obtener un archivo de íconos. MaxLength = 255
6. Haga clic en el botón **Continuar**.
7. Haga clic en **Listo**.
8. Haga clic en **Continuar**.
9. Haga clic en **Listo**.

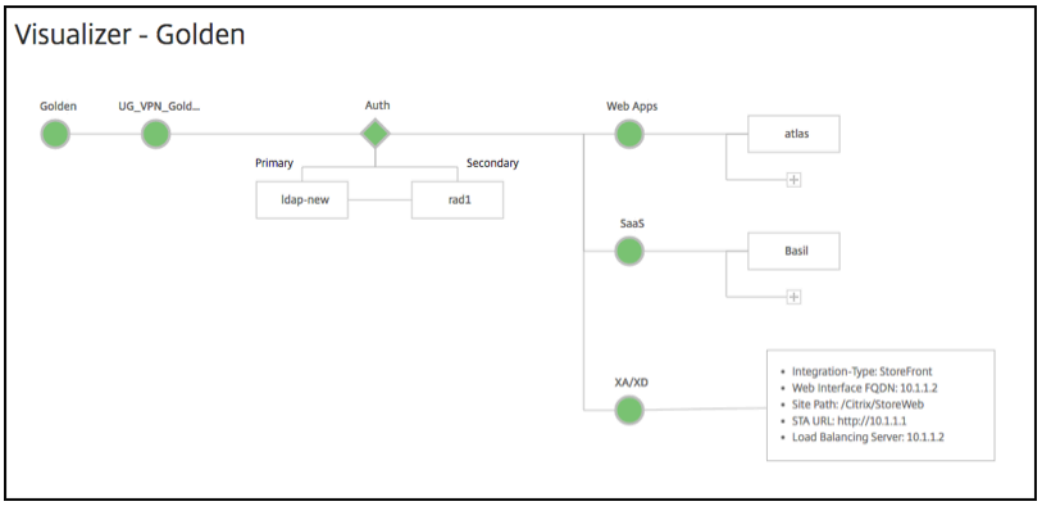
Configuración GUI

1. Seleccione Unified Gateway en el menú.

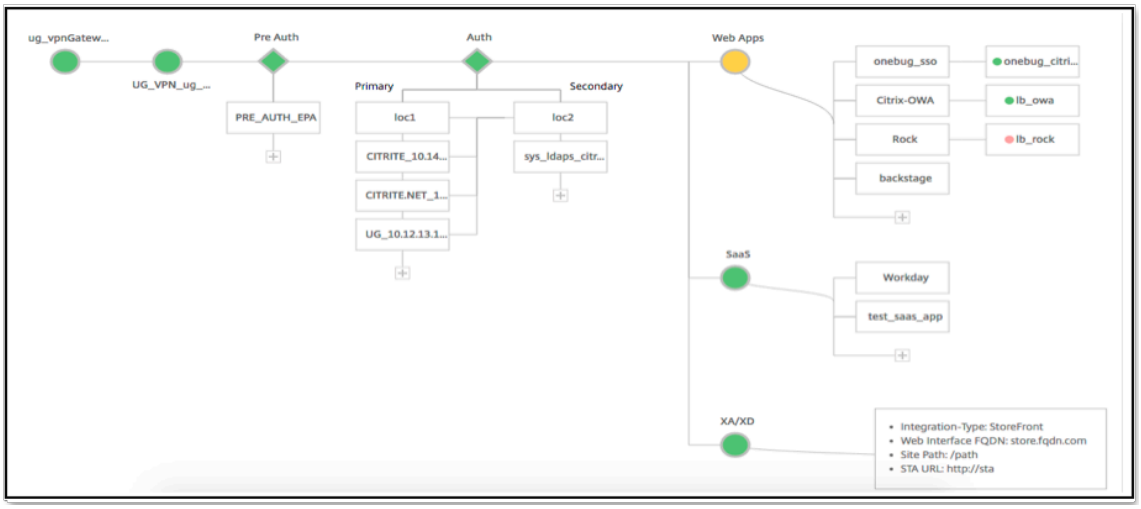
2. Haga clic en el icono del **visualizador de Unified Gateway** para acceder a instancias configuradas de Gateway.



El visualizador de Unified Gateway tiene el aspecto de un diagrama de flujo, como se muestra en la siguiente imagen:



El visualizador de Unified Gateway tiene PreAuth y una sección de aplicaciones. `Auth` Si el servidor virtual de VPN tiene una directiva de autenticación previa, solo entonces `pre-auth` se muestra en el visualizador de Unified Gateway.



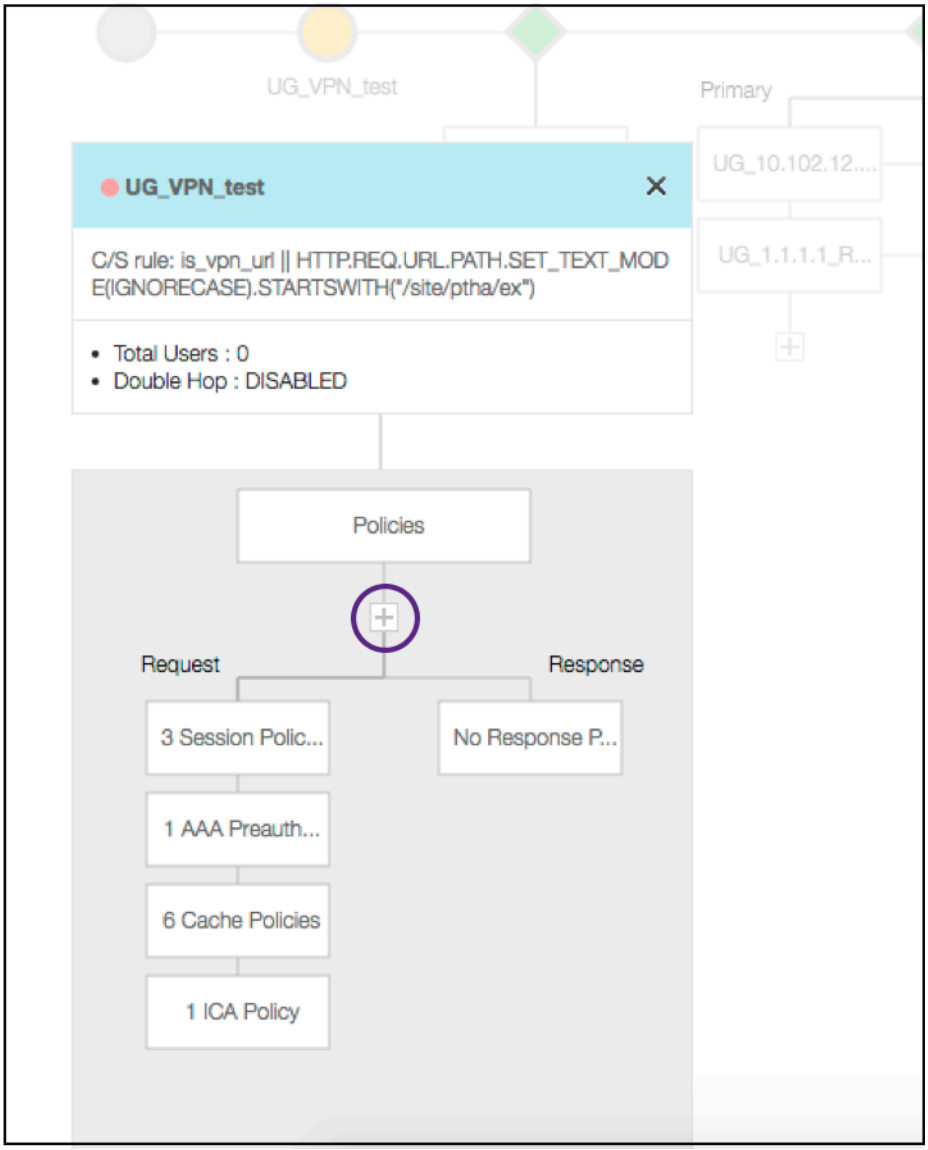
El visualizador de Unified Gateway utiliza un esquema de codificación de colores para el equilibrio de carga y los servidores virtuales VPN para indicar su estado.

Color	Descripción
Rojo	significa que el servidor está caído.
Gris	significa que las aplicaciones web/Citrix Virtual Apps no se han configurado.
Verde	significa que todo va bien con el servidor virtual.
Naranja	significa que uno de los servicios de servidor virtual de equilibrio de carga. está inactivo, pero sigue funcionando correctamente.

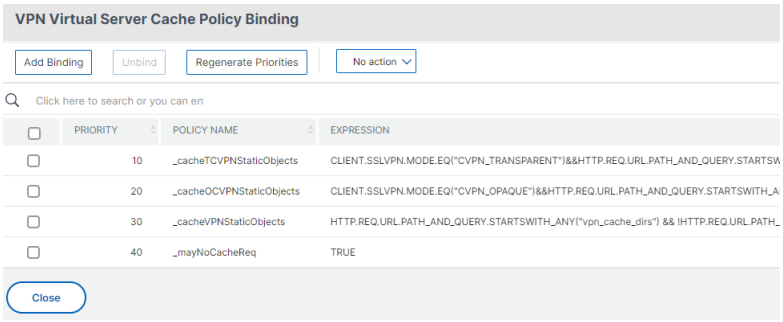
Detalles de los servidores virtuales VPN

Para obtener los detalles de los servidores virtuales VPN, haga clic en el **nodo Servidores virtuales VPN**. La ventana emergente representa detalles como la regla C/S y todas las directivas.

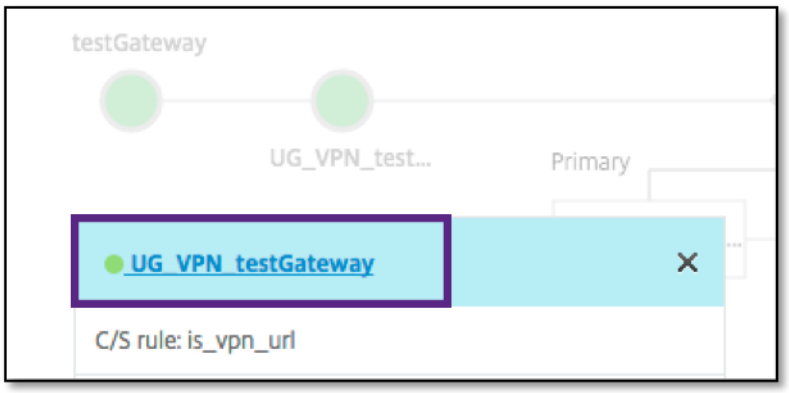
1. Agregue directivas a la entidad VPN haciendo clic en el icono (+).



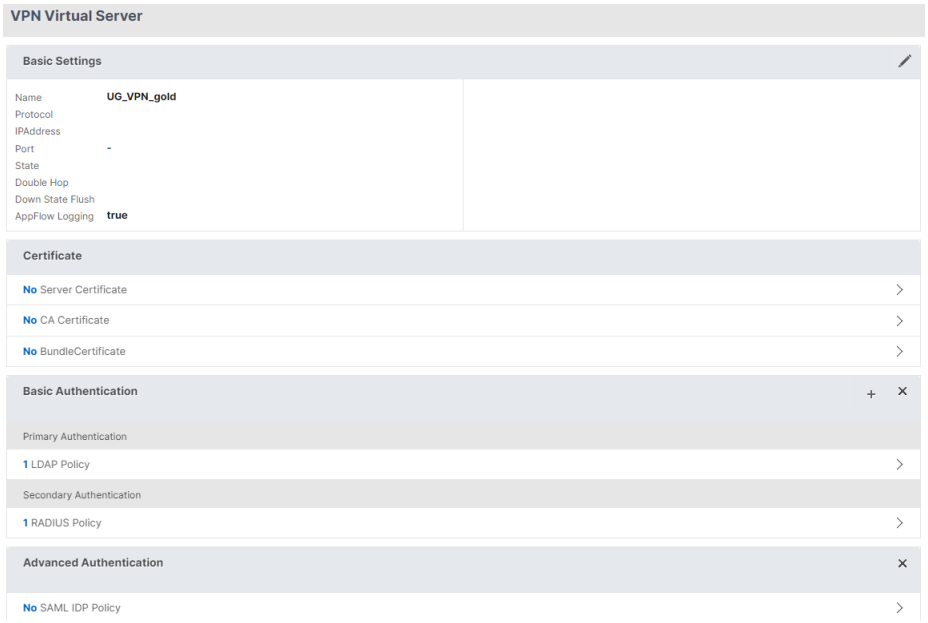
2. Haga clic en el nodo deseado para obtener detalles de las directivas ya configuradas.



Para obtener información sobre el servidor virtual de VPN, el título de VPN en la ventana emergente es una entidad en la que se puede hacer clic y que va a un control deslizante que detalla el servidor virtual de VPN.



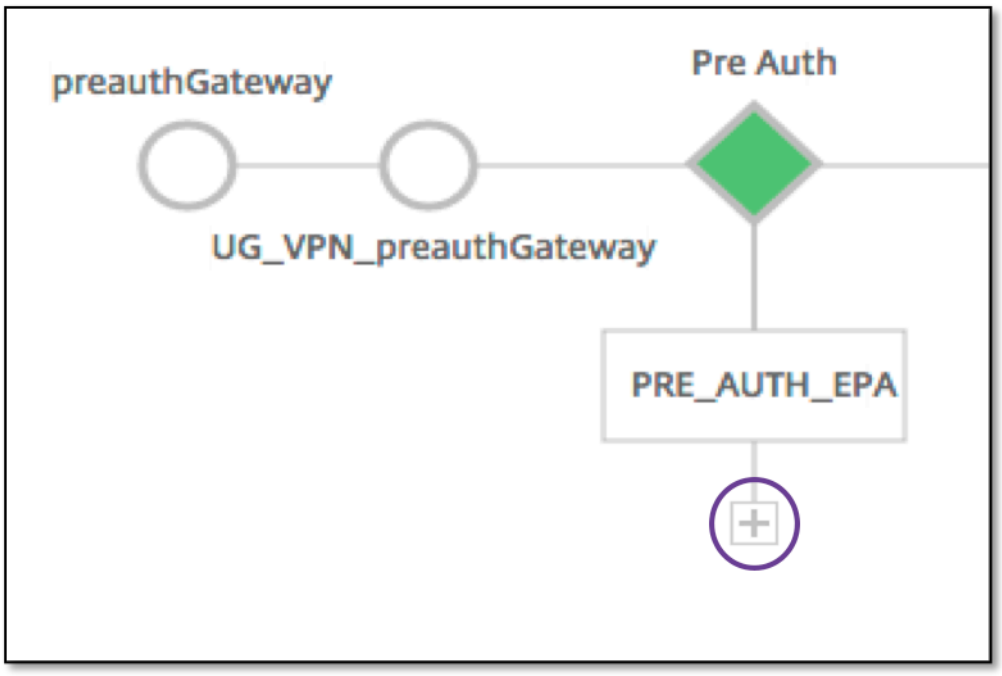
Los detalles del servidor VPN se muestran aquí.



The Pre Auth Block

Si un servidor virtual de VPN tiene directivas de autenticación previa asociadas, el visualizador de Unified Gateway muestra un bloque `Pre Auth`. El bloque `Pre Auth` muestra las directivas y ofrece una opción para agregar directivas de autenticación previa a la VPN.

1. Haga clic en el signo **+** para agregar una directiva `preauth`.

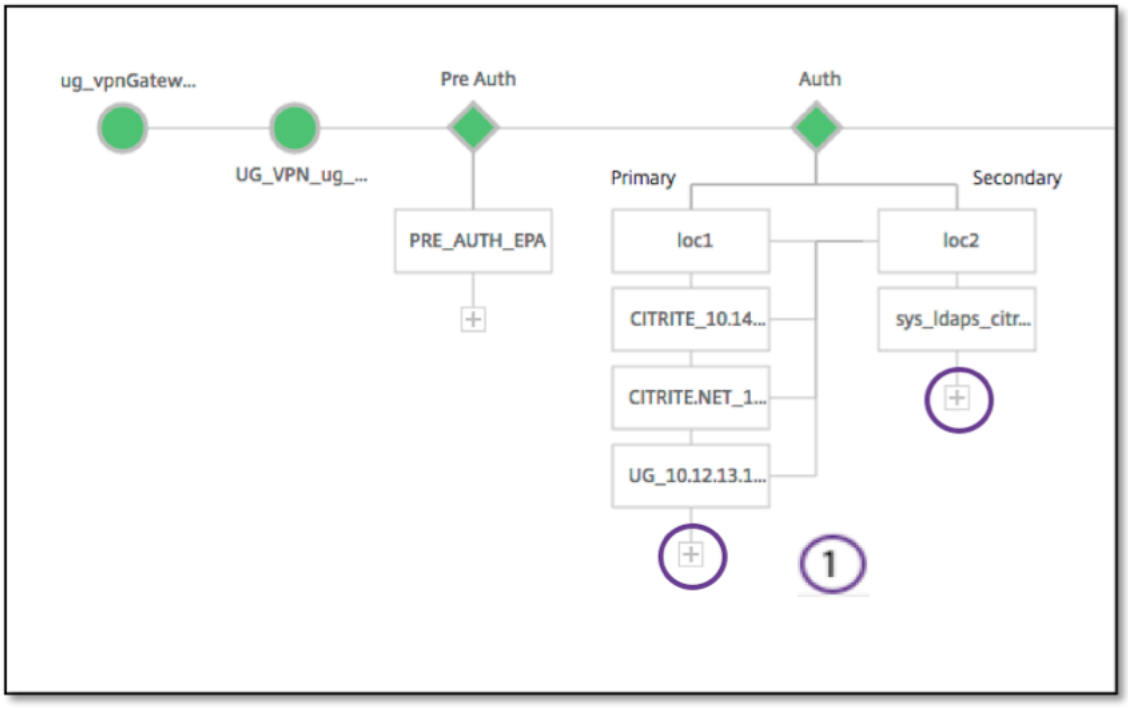


En caso de que no haya directivas de autenticación previa asociadas, este bloque se ocultaría de la vista.

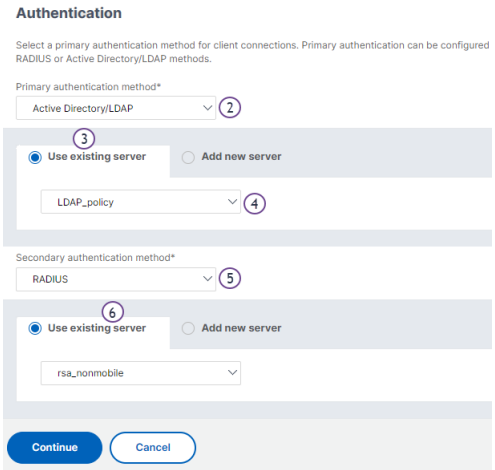
The Auth Block

El bloque `Auth` enumera las directivas principales y secundarias. El bloque `Auth` proporciona una opción para agregar directivas.

1. Haga clic en **+** en la lista Principal para agregar un enlace de autenticación principal o haga clic en + en la lista Secundaria para agregar un enlace de autenticación secundaria.

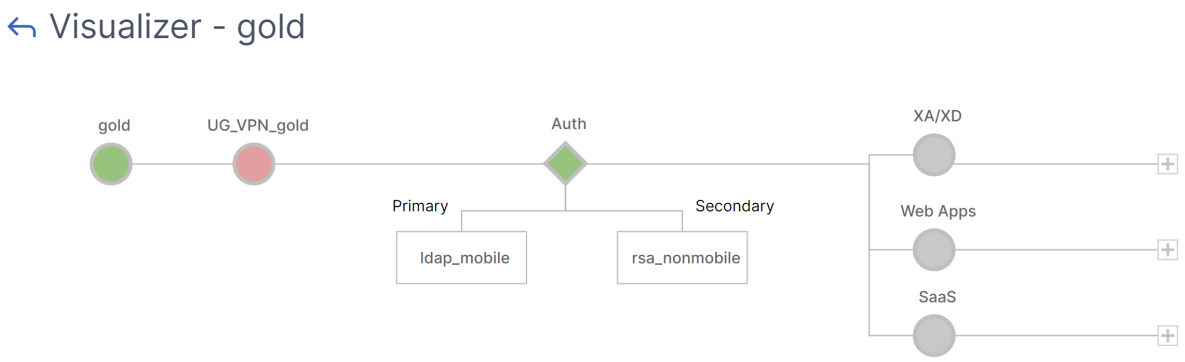


2. Seleccione una opción del menú **Método de autenticación principal**.
3. Especifique si es un **servidor existente** o **Agregar nuevo servidor** seleccionando el botón de opción.
4. Seleccione una opción del menú **Nombre de directiva LDAP**.
5. Seleccione **RADIUS** en el menú **Método de autenticación secundaria**.
6. Especifique si desea**utilizar el servidor existente** o **Agregar nuevo servidor** seleccionando el botón de opción.
7. Haga clic en **Continuar**.



Agregar StoreFront

1. Haga clic en **+** cerca de la XA/XD y le llevará a agregar aplicaciones "XA/XD".



Puede elegir su punto de integración. Las opciones son StoreFront, WI o WionNS. Haga clic en **Continuar**.

1. Complete los campos siguientes para configurar StoreFront. Los campos que requieren información obligatoria se indican con el *.

Campo	**Descripción**
—	—
FQDN* de StoreFront	Introduzca el FQDN del servidor de StoreFront. Longitud máxima: 255 char.Ejemplo: //storefront.xendt.net
Ruta del sitio*	Introduzca la ruta de acceso a Receiver para el sitio web ya configurado en StoreFront.
`Single Sign-on Domain`*	Introduzca el dominio predeterminado para la autenticación de usuarios
Nombre del almacén*	Escriba el nombre de los monitores StoreFront.
STORENAME es un argumento que define el nombre del almacén de servicios de StoreFront para sondear el estado de los servidores StoreFront. Aplicable a monitores StoreFront. Longitud máxima: 31
Servidor de Secure Tíquet Authority *	Introduzca la URL de Secure Tíquet Authority, que suele estar presente en el controlador de entrega.
Ejemplo:`http://sta`
StoreFront Server*	Introduzca la dirección IP del servidor de StoreFront
Protocolo	*Introduzca el protocolo utilizado por el servidor.*
Puerto	Introduzca el puerto utilizado por el servidor.
Equilibrio de carga	Introduzca la configuración de equilibrio de carga para los servidores de StoreFront.
Servidor virtual*	Introduzca la dirección IP pública para la implementación de Unified Gateway.

2. Haga clic en **Continuar.**

Adición de SaaS

1. Haga clic en **+** para agregar aplicaciones SaaS y le llevará a la página Agregar SaaS. Complete los campos siguientes para configurar SaaS. Los campos que requieren información obligatoria se indican con un*.

Campo	Descripción
Nombre*	Introduzca el nombre del enlace del marcador.
Tipo de aplicación	Introduzca el tipo de aplicación que representa esta URL de VPN.Los valores posibles son: Aplicación de intranet/acceso sin cliente/SaaS/aplicación preconfigurada en este NetScaler
Introduzca la URL*	Introduzca la URL de la aplicación de intranet.
Elegir **archivo**	Introduzca la URL para obtener el archivo de iconos para mostrar este recurso. MaxLength = 255

Incorporación de aplicaciones web

1. Haga clic en **+** para agregar aplicaciones web y le llevará a la página Agregar aplicaciones web. Complete los siguientes campos para configurar una aplicación web. Los campos que requieren información obligatoria se indican con un *.

Campo	Descripción
Nombre*	Introduzca el nombre del enlace del marcador.
Tipo de aplicación	Introduzca el tipo de aplicación que representa esta URL de VPN.Los valores posibles son: Aplicación de intranet/acceso sin cliente/SaaS/aplicación preconfigurada en este NetScaler
Introduzca la URL*	Introduzca la URL de la aplicación de intranet.

Campo	Descripción
Elegir **archivo**	Introduzca la URL para obtener el archivo de iconos para mostrar este parámetro resource.maxLength = 255

Si se puede acceder a una aplicación a través de la URL de Unified Gateway, se puede acceder a los detalles del servidor de equilibrio de carga haciendo clic en la aplicación:

Se pueden agregar nuevas directivas haciendo clic en (+) y todas las directivas vinculadas se pueden ver haciendo clic en el nodo que muestra la información de la directiva.

También se muestra el número de servicios vinculados al equilibrador de carga, junto con la información general del estado. Haga clic en una lista de todos los servicios. Se pueden agregar nuevos servicios al equilibrador de carga.

Para obtener más información sobre el equilibrador de carga, se puede hacer clic en el título de la ventana emergente que llega a la página de detalles del servidor virtual de equilibrio de carga.

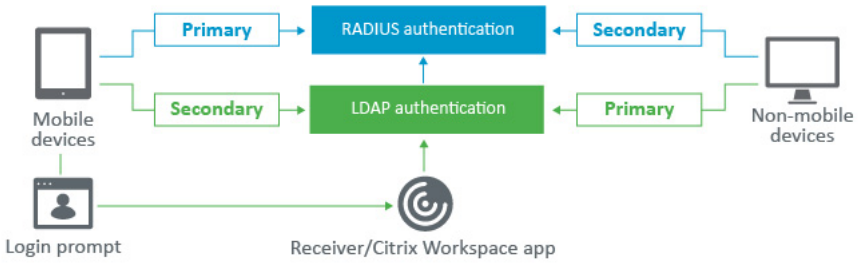
Configurar NetScaler Gateway para utilizar la autenticación RADIUS y LDAP con dispositivos móviles/tabletas

January 26, 2024

En esta sección se describe cómo configurar el dispositivo NetScaler Gateway para que utilice la autenticación RADIUS como principal y la autenticación LDAP como secundaria con dispositivos móviles o tabletas.

La configuración que se muestra en la sección permite que todas las demás conexiones utilicen primero LDAP y RADIUS en segundo lugar.

Al configurar la autenticación de dos factores en la aplicación Citrix Workspace para utilizarla con dispositivos móviles o tabletas, debe agregar el RSA SecureID (autenticación RADIUS) como autenticación principal. Pero cuando los usuarios reciben la solicitud de nombre de usuario y contraseña, código de acceso en Receiver, ponen primero LDAP y RADIUS como segundas credenciales. Desde el punto de vista del administrador, es una configuración diferente en comparación con una configuración no móvil.



Complete el procedimiento siguiente para configurar el dispositivo NetScaler Gateway para que utilice la autenticación RADIUS como principal y la autenticación LDAP como secundaria con dispositivos móviles o tabletas.

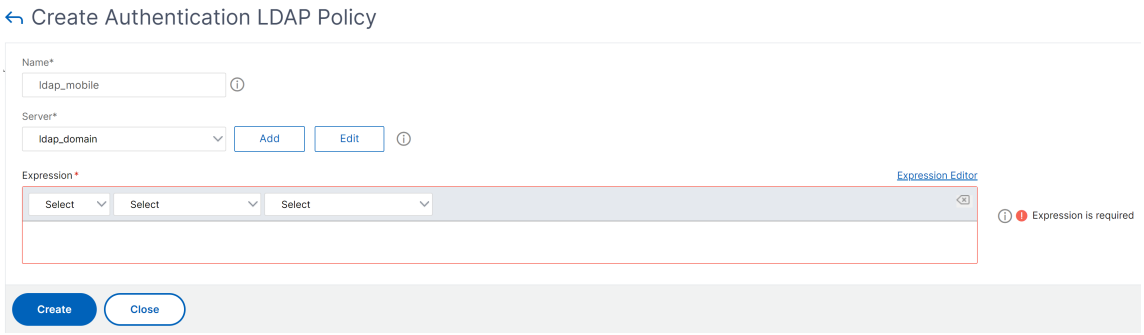
1. En la Utilidad de configuración, seleccione **NetScaler Gateway > Directivas > Autenticación** y cree una directiva de autenticación para LDAP y RSA para dispositivos móviles y no móviles. Esto es necesario para evitar una condición lógica que permita a los usuarios omitir la autenticación RADIUS.
2. Introduzca los detalles del servidor LDAP después de hacer clic en la opción **Agregar** de la ficha **Servidores** de LDAP.
3. Cree una directiva LDAP para los dispositivos móviles eligiendo el servidor LDAP necesario.

Para vincular esta directiva solo a dispositivos móviles, utilice la siguiente expresión:

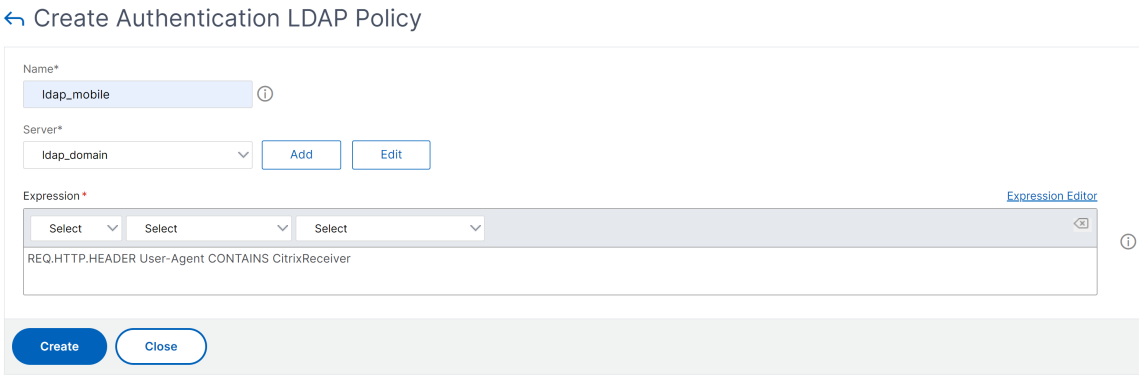
```
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
```

La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```

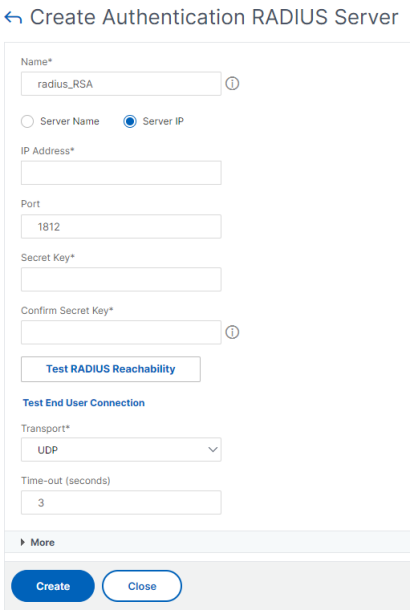


4. Haga clic en **Editor de expresiones** para crear una directiva:

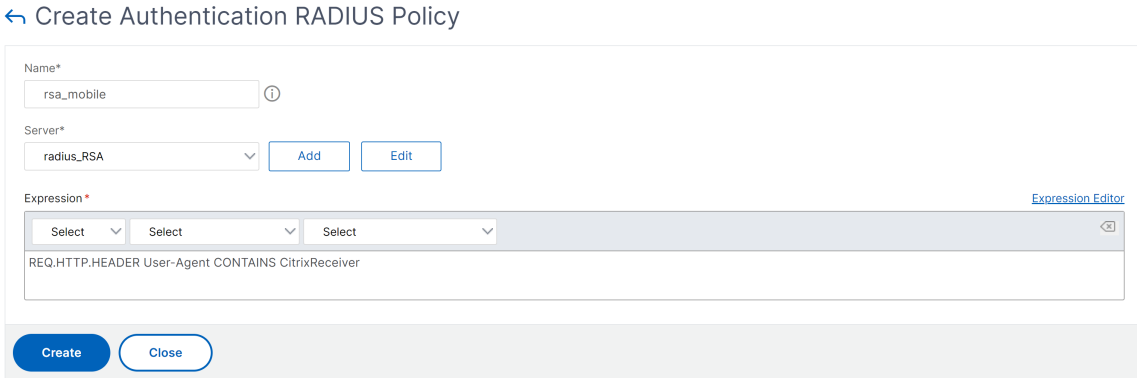


5. Cree una directiva RADIUS y un servidor RADIUS para los dispositivos móviles.

   - Vaya a la opción RADIUS desde **NetScaler Gateway > Directivas > Autenticación > RADIUS**. Haga clic en **Agregar** en la ficha Servidor.
   - Agregue los detalles necesarios. El puerto predeterminado para la autenticación RADIUS es 1812.



- Para vincular esta directiva solo a dispositivos móviles, utilice la siguiente expresión:

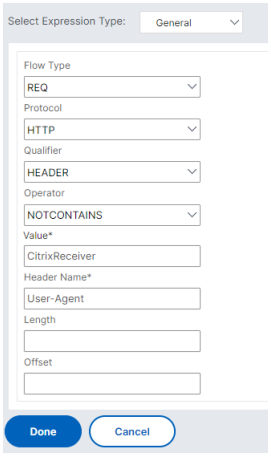


6. Siga el mismo paso para crear una directiva LDAP para dispositivos no móviles. Para vincular esta directiva solo a dispositivos no móviles, utilice la siguiente expresión:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

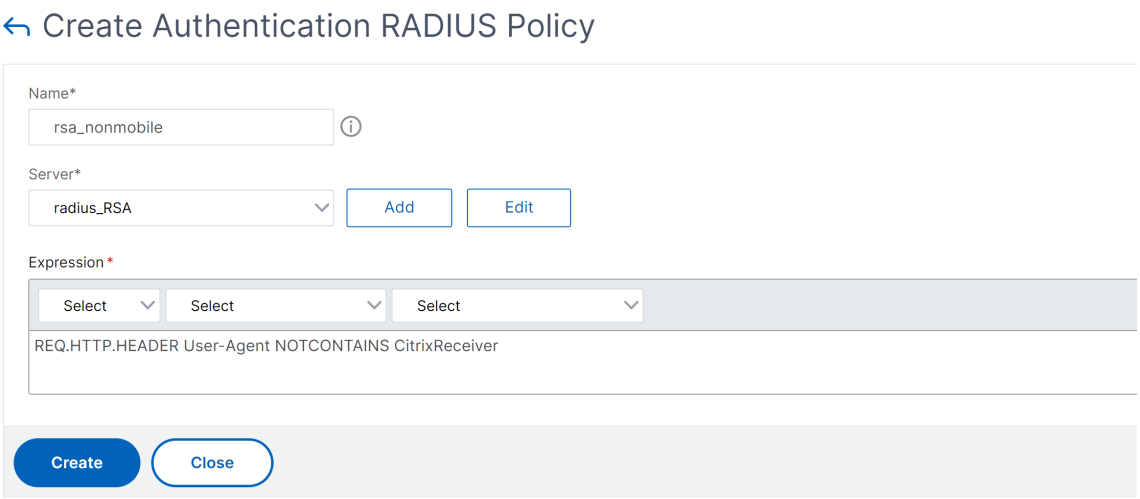



7. Cree una directiva RADIUS para dispositivos no móviles. Para vincular esta directiva solo a dispositivos no móviles, utilice la siguiente expresión:

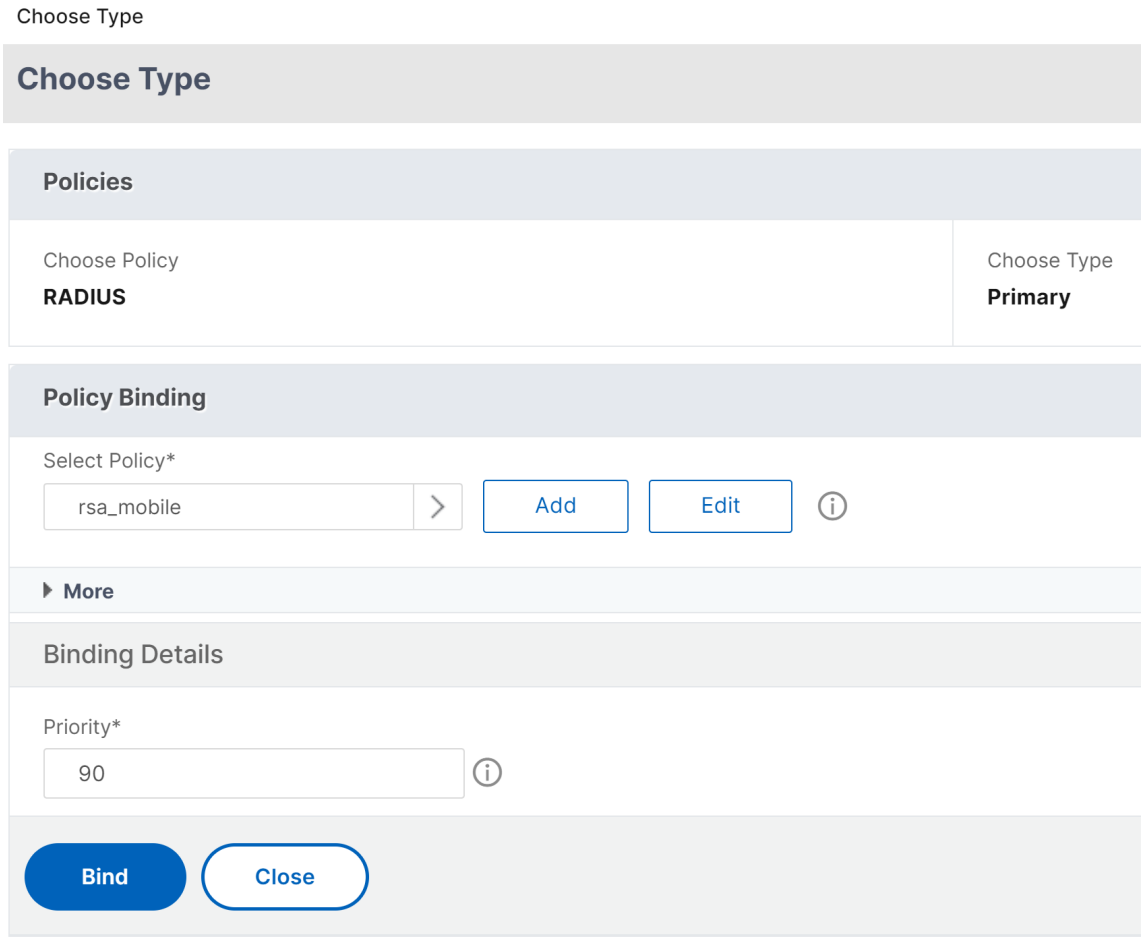
```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

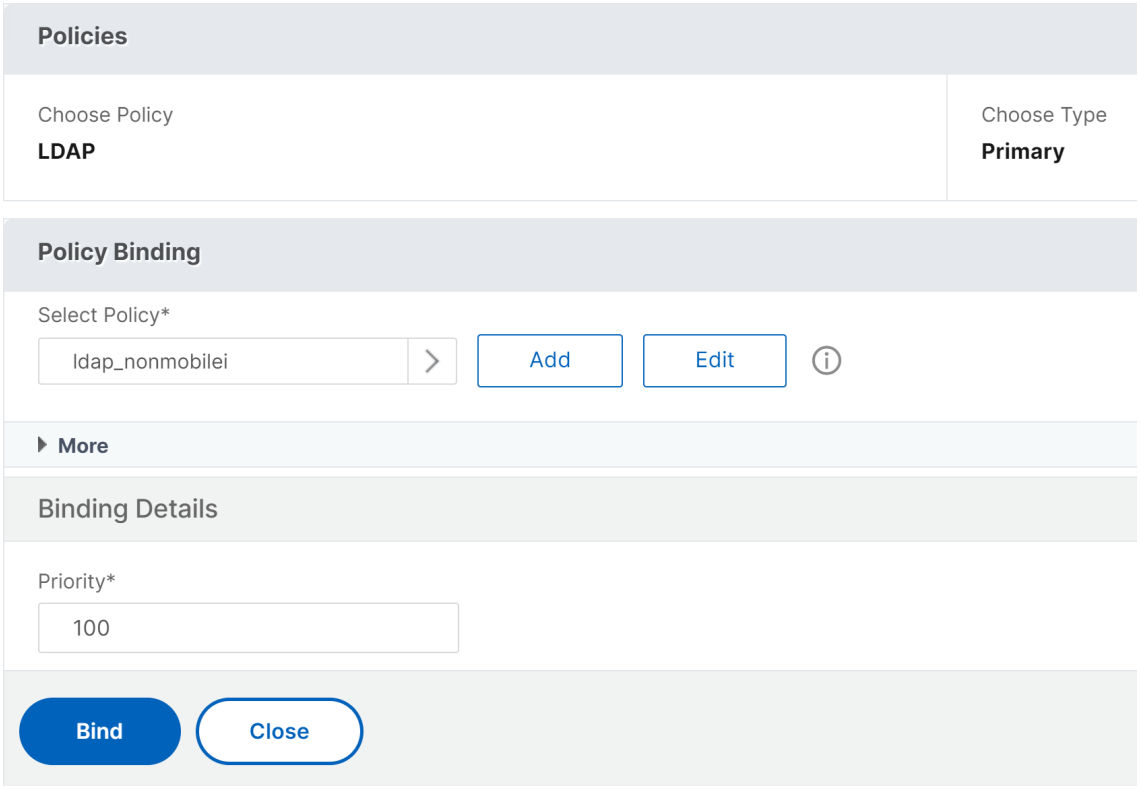
La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

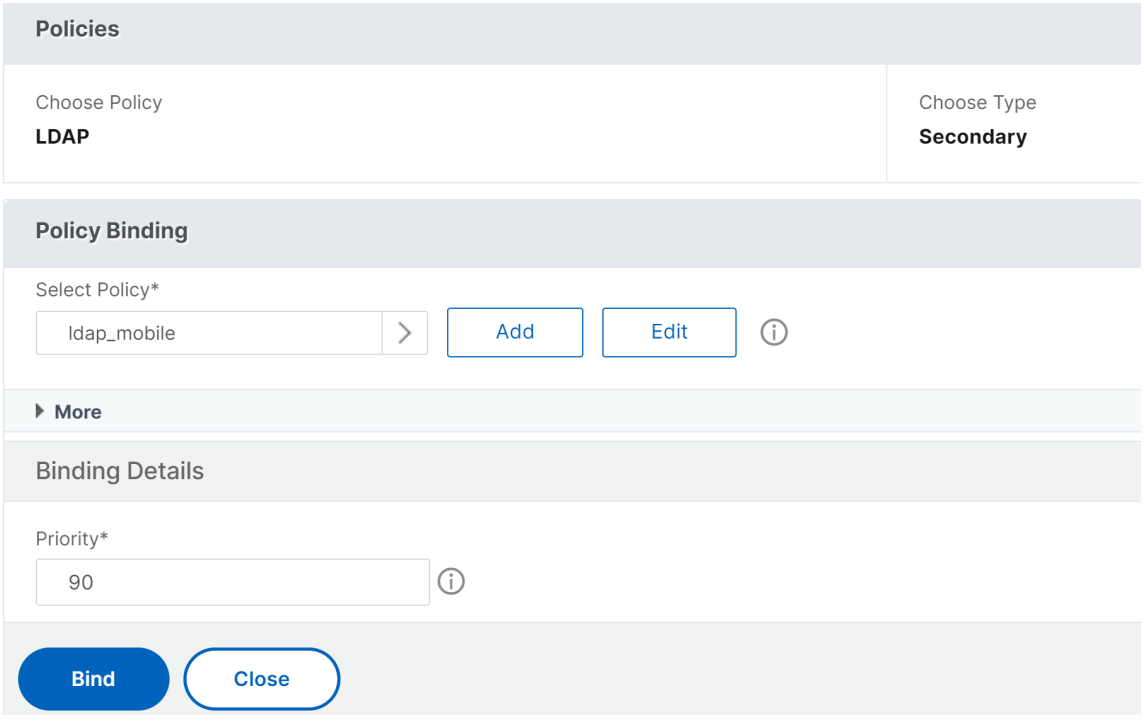


8. Vaya a Propiedades del servidor virtual de NetScaler Gateway y haga clic en la ficha **Autenticación**. En las directivas de autenticación principal, agregue la directiva RSA_mobile como prioridad máxima y la directiva LDAP_NonMobile como prioridad secundaria:





9. En las directivas de autenticación secundaria, agregue la directiva LDAP_mobile como prioridad máxima, seguida de la directiva RSA_nonMobile como prioridad secundaria:

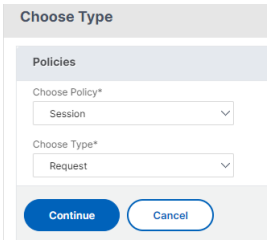


> La directiva de sesión debe tener el índice de credenciales de inicio de sesión único correcto, es decir, deben ser las credenciales LDAP. Para dispositivos móviles, el **índice de credenciales** en **Perfil de sesión > Experiencia del cliente** debe establecerse en **Secundario**, que es LDAP.

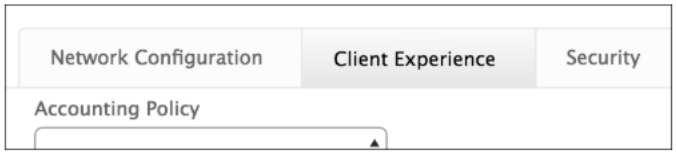
Por lo tanto, necesita dos directivas de sesión, una para dispositivos móviles y otra para dispositivos no móviles.

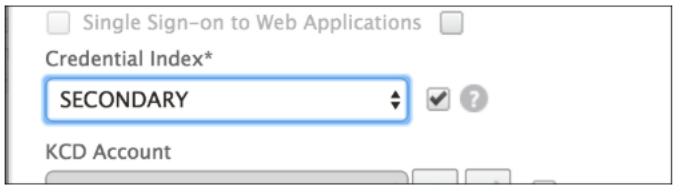
- En el caso de los dispositivos móviles, la directiva de sesión y el perfil de sesión aparecen tal y como se muestran en la siguiente captura de pantalla.
  Para crear una directiva de sesión, vaya a el servidor virtual necesario y, a continuación, haga clic en **Modificar**, vaya a la sección de directivas y haga clic en signo +:

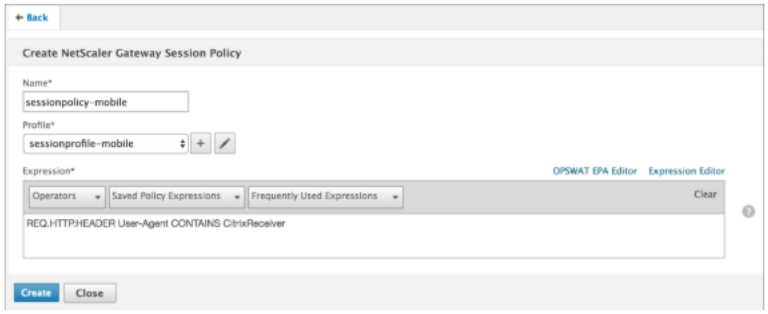
- Seleccione la opción **Sesión** del menú.



- Introduzca el nombre de la directiva de sesión que quiera y haga clic en + para crear un perfil. Para dispositivos móviles, el **índice de credenciales** en **Perfil de sesión > Experiencia del cliente** debe establecerse en **Secundario**, que es LDAP.







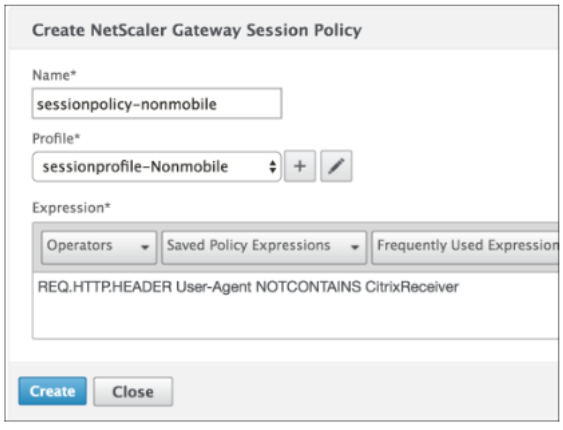
- Para dispositivos que no sean móviles, sigue los mismos pasos. **El índice de credenciales** en **Perfil de sesión > Experiencia del cliente** debe establecerse en **Principal**, que es LDAP.

La expresión debe cambiarse a:

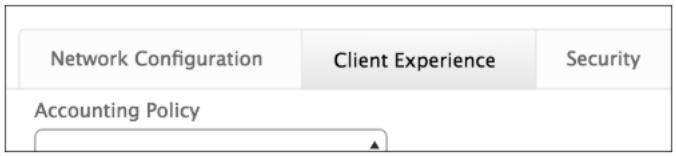
```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

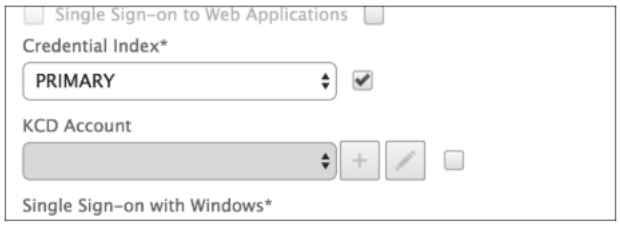
La expresión avanzada correspondiente es:

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

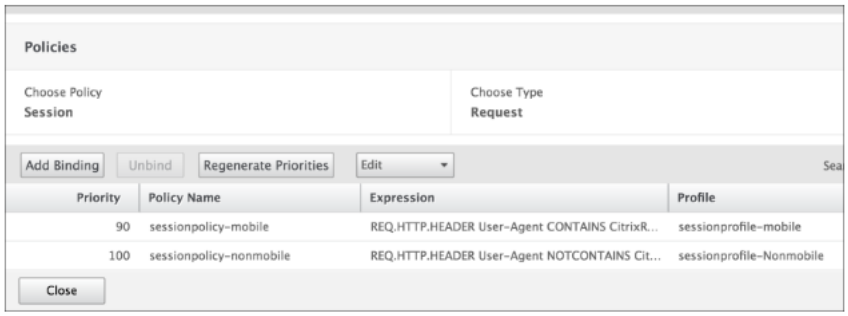


- Para crear un perfil para usuarios que no son móviles, haga clic en signo +.

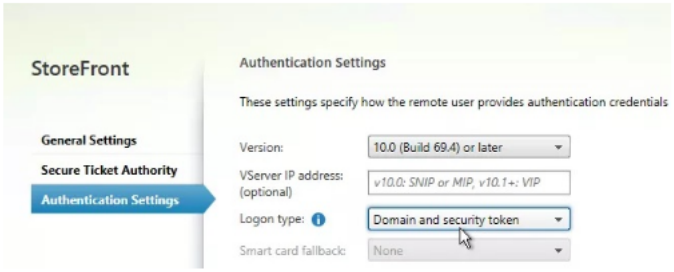


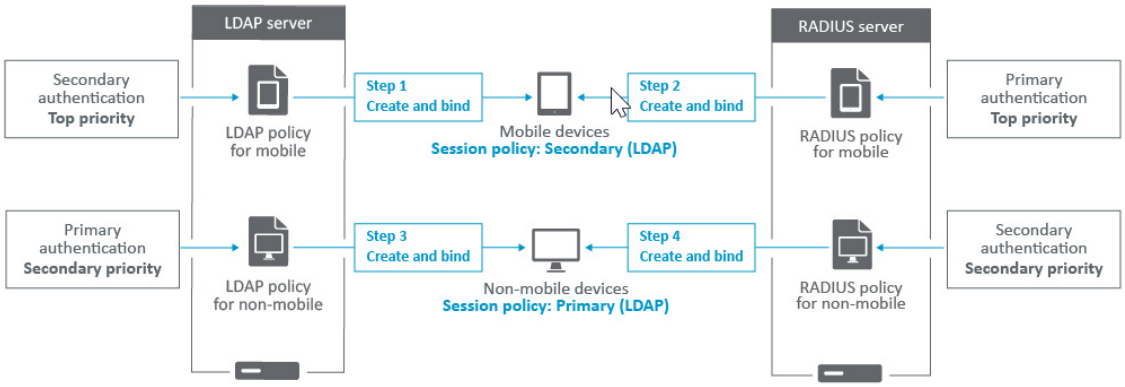


10. En la siguiente ilustración se muestran las directivas y los perfiles del servidor virtual necesario.



11. También en StoreFront, en la configuración de NetScaler Gateway establecida para usar "Tipo de inicio de sesión"= "Dominio y token de seguridad"





Restringir el acceso a NetScaler Gateway para los miembros de un grupo de Active Directory

March 27, 2024

NetScaler Gateway admite dos métodos para restringir el acceso de inicio de sesión.

- Filtro de búsqueda LDAP: solo los nombres de usuario que coinciden con el filtro de búsqueda LDAP (por ejemplo, pertenencia a grupos de Active Directory) pueden iniciar sesión en NetScaler Gateway.
- Grupos con permiso para iniciar sesión en un perfil o directiva de sesión de NetScaler Gateway: este método admite varios grupos de Active Directory. Para obtener información detallada, consulte https://support.citrix.com/article/CTX125797.

En este artículo se describe el método del filtro de búsqueda LDAP.

Información general

Cuando un usuario introduce las credenciales en la página de inicio de sesión del servidor virtual de NetScaler Gateway y presiona ENTRAR, el dispositivo busca primero el nombre de usuario en Active Directory (LDAP). Si no se ha definido un filtro de búsqueda LDAP en la directiva LDAP ni en el servidor, el dispositivo busca una coincidencia en todos los nombres de usuario de Active Directory. Una vez que se encuentra una coincidencia, el dispositivo extrae el nombre distintivo (DN) completo del usuario y utiliza el DN y la contraseña del usuario para autenticarse en Active Directory.

Si se define un filtro de búsqueda LDAP, solo se buscarán coincidencias de nombres de usuario que coincidan con el filtro de búsqueda LDAP. Por ejemplo, si el filtro de búsqueda LDAP se crea para buscar solo miembros de un grupo de Active Directory, el nombre de usuario introducido por el usuario debe coincidir con los miembros del grupo.

Requisitos previos

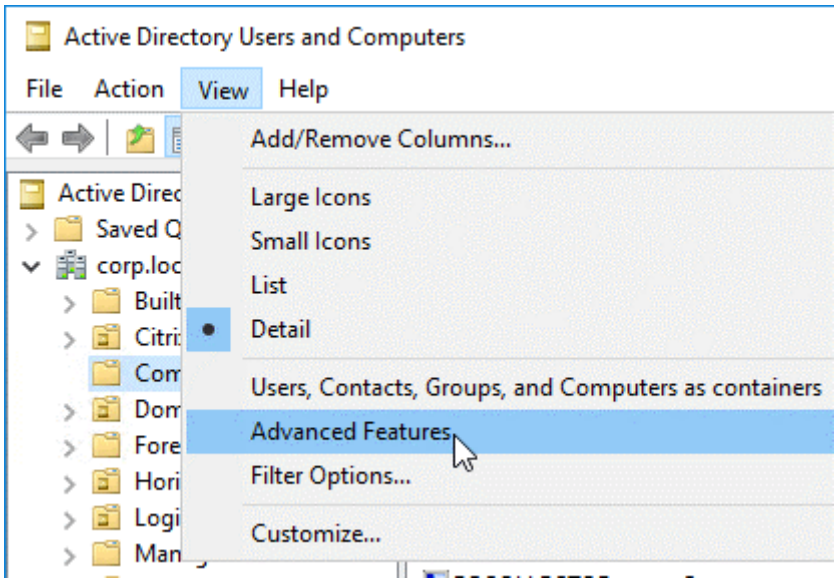
El servidor virtual NetScaler Gateway debe estar configurado para la autenticación LDAP.

Pasos para configurar un filtro de búsqueda LDAP para los miembros de un grupo de Active Directory

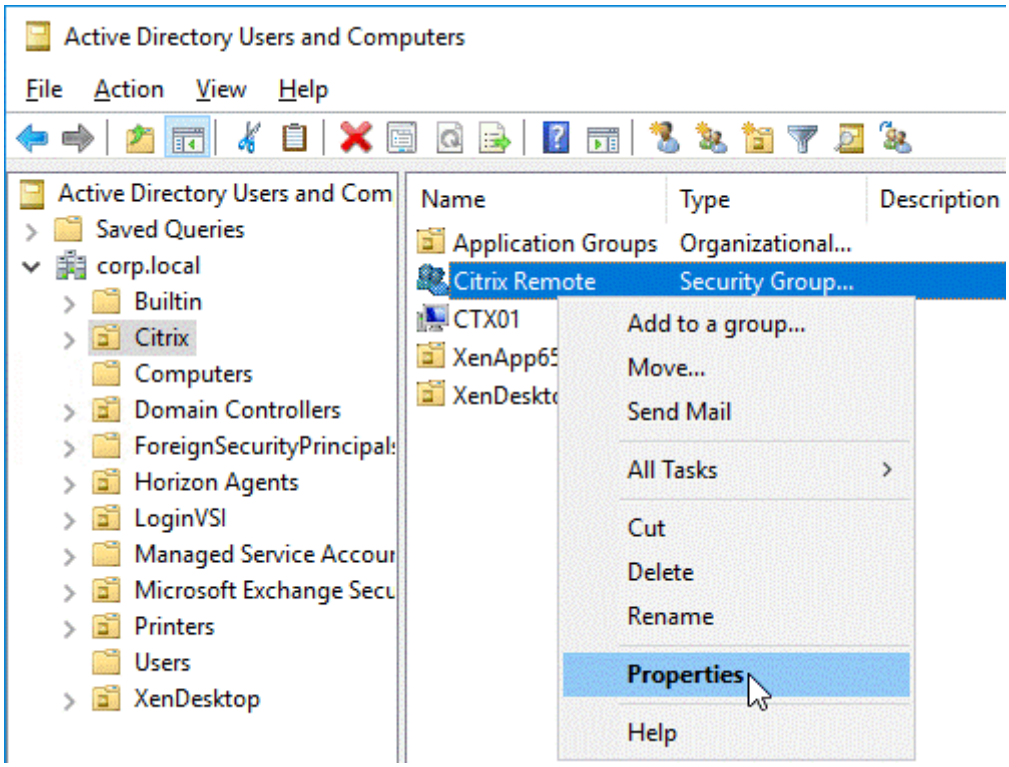
1. Determine el grupo de Active Directory que tiene permiso de acceso y obtenga su nombre distintivo completo.

Una forma sencilla de obtener el nombre distintivo completo del grupo es a través de Usuarios y equipos de Active Directory.

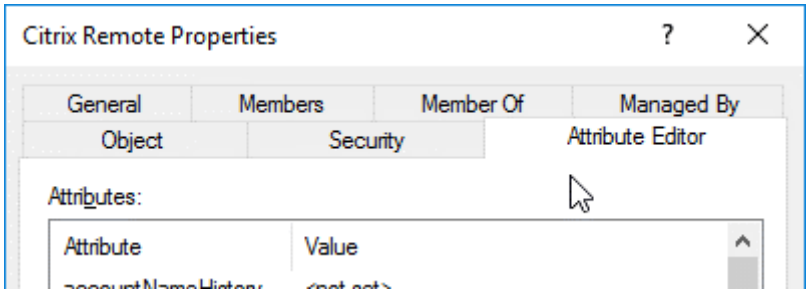
2. En Usuarios y equipos de Active Directory, en el menú **Ver**, active **Funciones avanzadas**.



3. Examine el árbol hasta el objeto de grupo, haga clic con el botón secundario del mouse y, a continuación, haga clic en **Propiedades**.
Nota: No puede usar **Buscar**. En su lugar, debe navegar por el árbol para encontrar el objeto.

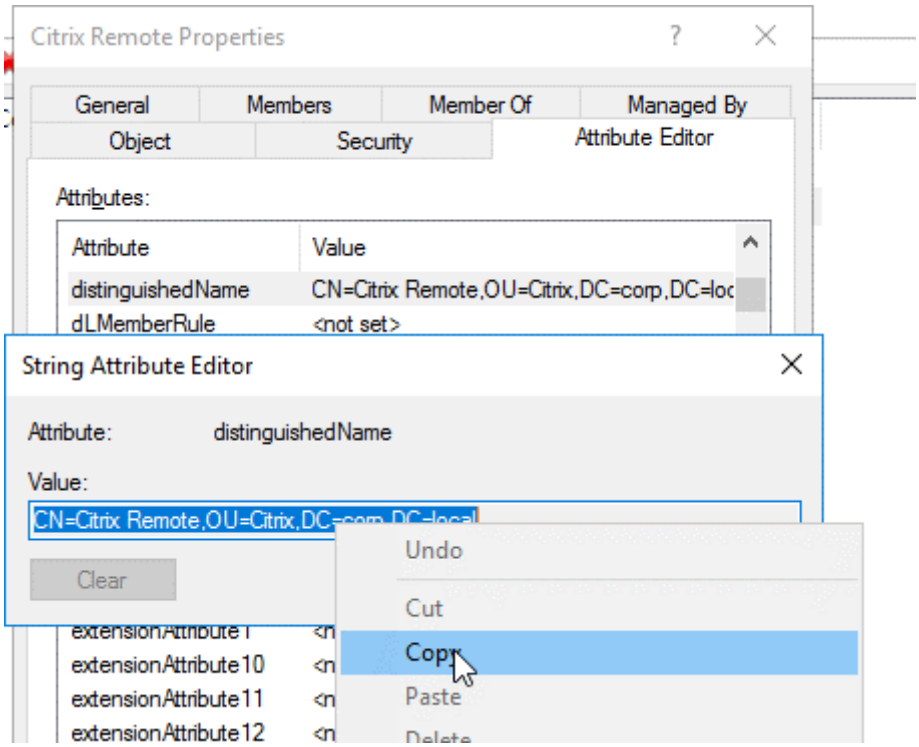


4. A la derecha, cambia a la ficha **Editor de atributos**.

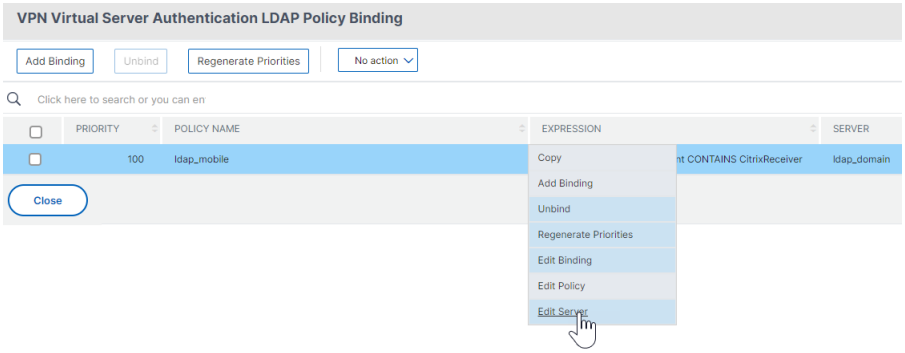


Esta ficha solo está visible si **las funciones avanzadas** están habilitadas y si no ha utilizado la función **Buscar**.

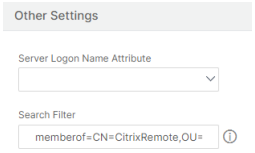
5. Vaya hacia abajo hasta **distinguishedName**, haga doble clic en él y, a continuación, cópielo en el portapapeles.



6. En la GUI de NetScaler Gateway, vaya a **NetScaler Gateway > Servidores virtuales**.
7. Seleccione un servidor virtual NetScaler Gateway existente y haga clic en **Modificar**.
8. En la sección Autenticación básica, haga clic en **Directivas LDAP**.
9. Haga clic con el botón secundario del mouse en una directiva LDAP existente y haga clic en **Modificar servidor**.



10. En la sección **Otros ajustes**, en el campo **Filtro de búsqueda**, escriba **memberOf=** y, a continuación, pegue el nombre distintivo del grupo de Active Directory después del signo igual (=).



Un ejemplo de filtro de búsqueda es el siguiente:
memberOf=CN=Citrix Remote, OU=Citrix, DC=corp, DC=local
Nota: De forma predeterminada, NetScaler solo busca nombres de usuario que sean miembros directos del grupo de Active Directory. Si quiere buscar grupos anidados, agregue Microsoft OID al filtro de búsqueda LDAP. El OID se inserta entre memberOf y =.

Ejemplo: memberOf:1.2.840.113556.1.4.1941:=CN=Citrix Remote, OU=Citrix, DC=corp, DC=local

11. Haga clic en **Aceptar**.

Usar la alta disponibilidad

January 26, 2024

Una implementación de alta disponibilidad de dos dispositivos NetScaler Gateway puede proporcionar un funcionamiento ininterrumpido en cualquier transacción. Al configurar un dispositivo como nodo principal y el otro como nodo secundario, el nodo principal acepta conexiones y administra los servidores, mientras que el nodo secundario supervisa el principal. Si, por cualquier motivo, el nodo principal no puede aceptar conexiones, el nodo secundario asume el control.

El nodo secundario supervisa el principal mediante el envío de mensajes periódicos (a menudo denominados mensajes de latidos o comprobaciones de estado) para determinar si el nodo principal acepta conexiones. Si se produce un error en una comprobación de estado, el nodo secundario vuelve a intentar la conexión durante un período especificado, tras el cual determina que el nodo principal

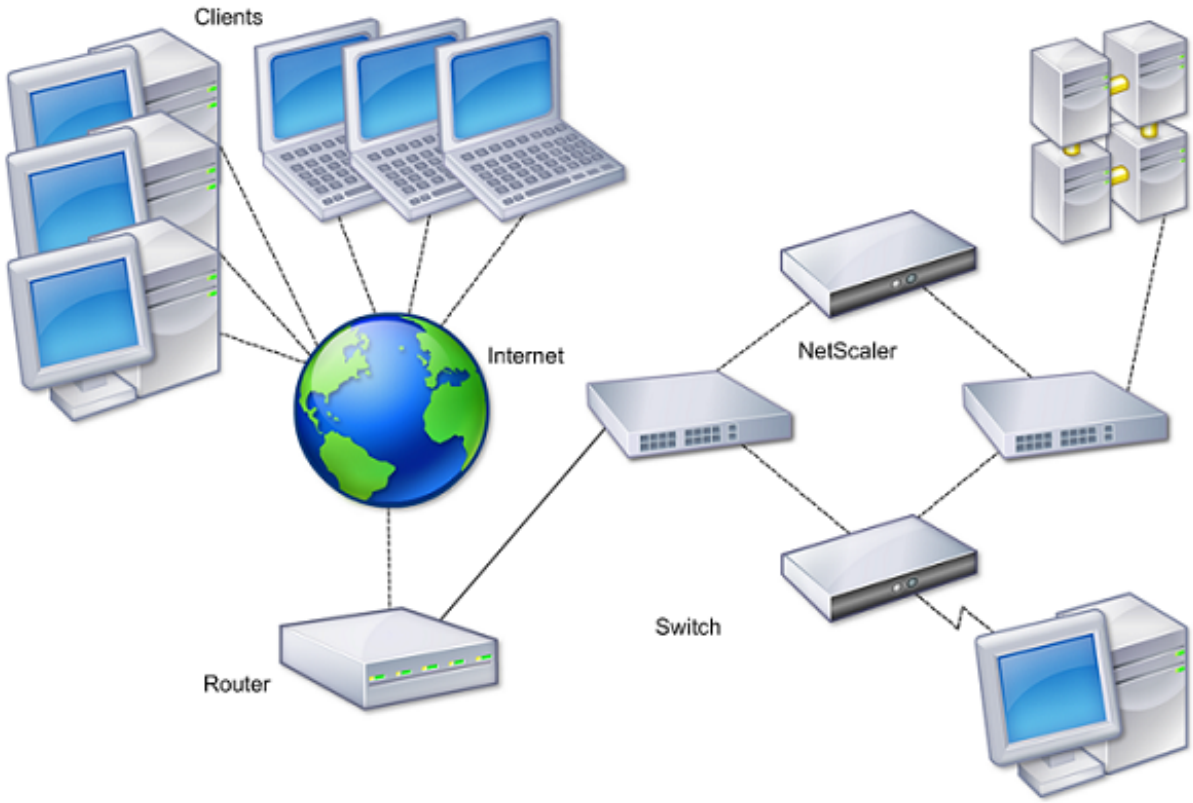
no funciona con normalidad. A continuación, el nodo secundario asume el control del principal (un proceso denominado conmutación por error).

Tras una conmutación por error, todos los clientes deben restablecer sus conexiones con los servidores administrados, pero las reglas de persistencia de sesiones se mantienen como antes de la conmutación por error.

Con la persistencia de registro del servidor web habilitada, no se pierden datos de registro debido a la conmutación por error. Para habilitar la persistencia de registros, la configuración del servidor de registros debe incluir entradas para ambos sistemas en el archivo log.conf.

En la siguiente ilustración se muestra una configuración de red con un par de alta disponibilidad.

Figura 1. Dispositivos NetScaler Gateway en una configuración de alta disponibilidad



Los pasos básicos para configurar la alta disponibilidad son los siguientes:

1. Cree una configuración básica, con ambos nodos en la misma subred.
2. Personalice los intervalos en los que los nodos comunican información de comprobación de estado.
3. Personalice el proceso mediante el cual los nodos mantienen la sincronización.
4. Personaliza la propagación de comandos del principal al secundario.
5. De forma opcional, configure el modo a prueba de fallos para evitar una situación en la que ninguno de los nodos sea principal.

6. Configure direcciones MAC virtuales si su entorno incluye dispositivos que no aceptan mensajes ARP gratuitos de NetScaler Gateway.

Cuando esté preparado para una configuración más compleja, puede configurar nodos de alta disponibilidad en distintas subredes.

Para mejorar la fiabilidad de su configuración de alta disponibilidad, puede configurar monitores de rutas y crear enlaces redundantes. En algunas situaciones, como cuando se solucionan problemas o se realizan tareas de mantenimiento, es posible que quiera forzar la conmutación por error de un nodo (asignar el estado principal al otro nodo), o forzar que el nodo secundario permanezca secundario o que el nodo principal permanezca como principal.

Cómo funciona la alta disponibilidad

January 26, 2024

Al configurar NetScaler Gateway en un par de alta disponibilidad, el NetScaler Gateway secundario supervisa el primer dispositivo mediante el envío de mensajes periódicos, también denominados mensaje de latido o comprobación de estado, para determinar si el primer dispositivo acepta conexiones. Si se produce un error en la comprobación de estado, el NetScaler Gateway secundario vuelve a intentar la conexión durante un período de tiempo especificado hasta que determina que el dispositivo principal no funciona. Si el dispositivo secundario confirma el error de comprobación de estado, el NetScaler Gateway secundario se hace cargo del NetScaler Gateway principal. Esto se denomina conmutación por error.

Los siguientes puertos se utilizan para intercambiar información relacionada con la alta disponibilidad entre dispositivos NetScaler Gateway:

- El puerto UDP 3003 se utiliza para intercambiar paquetes de saludo para comunicar el estado de los intervalos.
- El puerto TCP 3010 se utiliza para la sincronización de la configuración de alta disponibilidad.
- El puerto TCP 3011 se utiliza para sincronizar los valores de configuración.

Directrices para configurar la alta disponibilidad

Antes de configurar un par de alta disponibilidad, debe revisar estas directrices:

- Cada dispositivo NetScaler Gateway debe ejecutar la misma versión del software NetScaler Gateway. Encontrará el número de versión en la parte superior de la página de la utilidad de configuración.

- NetScaler Gateway no sincroniza automáticamente contraseñas entre dos dispositivos. Puede configurar cada NetScaler Gateway con el nombre de usuario y la contraseña del otro dispositivo del par.
- Las entradas del archivo de configuración, ns.conf, tanto en el NetScaler Gateway principal como en el secundario deben coincidir, con las siguientes excepciones:
  - El dispositivo NetScaler Gateway principal y secundario deben configurarse con su propia dirección IP exclusiva del sistema. Utilice el Asistente de configuración para configurar o modificar la dirección IP del sistema en NetScaler Gateway.
  - En un par de alta disponibilidad, el ID de NetScaler Gateway y la dirección IP asociada deben apuntar al otro NetScaler Gateway.

    Por ejemplo, si tiene dos dispositivos, denominados AG1 y AG2, debe configurar AG1 con el ID y la dirección IP exclusivos de NetScaler Gateway de AG2. Debe configurar AG2 con el ID y la dirección IP exclusivos de NetScaler Gateway de AG1.

    Nota: Cada dispositivo NetScaler Gateway siempre se identifica como Nodo 0. Configure cada dispositivo con un ID de nodo único.
- Cada dispositivo del par de alta disponibilidad debe tener la misma licencia. Para obtener más información sobre las licencias, consulte Licencias.
- Si crea un archivo de configuración en cualquiera de los nodos mediante un método que no pasa directamente por la utilidad de configuración ni por la interfaz de línea de comandos (por ejemplo, importar certificados SSL o cambiar a scripts de inicio), debe copiar el archivo de configuración en el otro nodo o crear un archivo idéntico archivo en ese nodo.
- Al configurar un par de alta disponibilidad, asegúrese de que las direcciones IP asignadas y la dirección de puerta de enlace predeterminada del dispositivo principal y del dispositivo secundario sean idénticas. Si es necesario, puede cambiar la dirección IP asignada en cualquier momento ejecutando el Asistente de configuración.

Puede utilizar la lista de comprobación previa a la instalación para ver una lista de los ajustes específicos que necesita configurar en una implementación de alta disponibilidad. Para obtener más información, consulte Lista de comprobación previa a la instalación.

Configuración de los ajustes de alta disponibilidad

March 27, 2024

Para configurar una configuración de alta disponibilidad, debe crear dos nodos, cada uno de los cuales define la dirección IP de NetScaler Gateway del otro como nodo remoto. Para empezar, inicie sesión en uno de los dos dispositivos NetScaler que quiera configurar para obtener alta disponibilidad y agregar un nodo. Especifique la dirección IP de NetScaler Gateway del otro dispositivo como

dirección del nuevo nodo. A continuación, inicie sesión en el otro dispositivo y agregue un nodo que tenga la dirección IP de NetScaler Gateway del primer dispositivo. Un algoritmo determina qué nodo pasa a ser primario y cuál se convierte en secundario.

Antes de configurar los dispositivos, agregue un nodo de alta disponibilidad. Este nodo representa el primer o el segundo NetScaler Gateway del par de alta disponibilidad. Para configurar la alta disponibilidad, primero debe crear el nodo y, a continuación, configurar la configuración de alta disponibilidad.

Para agregar un nodo de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, en la ficha Nodos, haga clic en **Agregar**.
3. En la página **Crear nodo de alta disponibilidad**, en el cuadro de texto **Dirección IP del nodo remoto**, escriba la dirección NSIP del NetScaler que se va a agregar como nodo remoto. Si la dirección IP de NetScaler Gateway es una dirección IPv6, active la casilla de verificación **IPv6** antes de introducir la dirección.
4. Si quiere agregar el nodo local al nodo remoto automáticamente, seleccione Configurar sistema remoto para participar en la configuración de alta disponibilidad. Si no selecciona esta opción, debe iniciar sesión en el dispositivo representado por el nodo remoto y agregar el nodo que está configurando actualmente.
5. Haga clic para habilitar **Desactivar las interfaces/canales de HA Monitor que están inactivos**.
6. Si el dispositivo remoto tiene un nombre de usuario y una contraseña diferentes, en Credenciales de inicio de sesión del sistema remoto, haga clic en Las credenciales de inicio de sesión del sistema remoto son distintas del nodo propio.
7. En **Nombre de usuario**, escriba el nombre de usuario del dispositivo remoto.
8. En **Contraseña**, escriba la contraseña del dispositivo remoto.
9. Haga clic en **Aceptar**.

Para habilitar o inhabilitar el nodo secundario

Solo puede inhabilitar o habilitar el nodo secundario. Cuando inhabilita un nodo secundario, deja de enviar mensajes de latido al nodo principal y, por lo tanto, el nodo principal ya no puede comprobar el estado del nodo secundario. Al habilitar un nodo, el nodo forma parte de la configuración de alta disponibilidad.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.

2. En el panel de detalles, en la ficha Nodos, seleccione el nodo local y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo Configuración de nodo de HA, en Estado de alta disponibilidad, seleccione ACTIVADO (No participar en HA).
4. Haga clic en Aceptar. Aparece un mensaje en la barra de estado que indica que el nodo se ha configurado correctamente.

Para configurar los ajustes de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo **Configurar nodo de HA**, en ID, escriba el número del identificador del nodo. ID especifica el número de nodo exclusivo del otro dispositivo.
4. En **Dirección IP**, escriba la dirección IP del sistema y, a continuación, haga clic en Aceptar. La dirección IP especifica la dirección IP del otro dispositivo.

Nota: El identificador máximo para los nodos de un par de alta disponibilidad es 64.

Cambio de la contraseña de un nodo RPC

March 27, 2024

Para comunicarse con otros dispositivos NetScaler Gateway, cada dispositivo requiere conocer los demás dispositivos, incluido cómo autenticarse en NetScaler Gateway. Los nodos RPC son entidades internas del sistema utilizadas para la comunicación de información de configuración y sesión de sistema a sistema. Existe un nodo RPC en cada NetScaler Gateway y almacena información, como las direcciones IP del otro dispositivo NetScaler Gateway y las contraseñas utilizadas para la autenticación. El NetScaler Gateway que establece contacto con otro NetScaler Gateway comprueba la contraseña dentro del nodo RPC.

NetScaler Gateway requiere contraseñas de nodo RPC en ambos dispositivos en un par de alta disponibilidad. Las contraseñas deben ser las mismas en ambos dispositivos. El dispositivo principal debe conocer la contraseña del nodo RPC secundario y el secundario debe conocer la contraseña del nodo RPC principal. Inicialmente, cada NetScaler Gateway se configura con la misma contraseña de nodo RPC. Para mejorar la seguridad, debe cambiar las contraseñas de nodo RPC predeterminadas. Puede utilizar la utilidad de configuración para configurar y cambiar nodos RPC.

Los nodos RPC se crean implícitamente al agregar un nodo o agregar un sitio de equilibrio de carga de servidor global (GSLB). No se pueden crear ni eliminar nodos RPC manualmente.

> **Importante:**
>
> También debe proteger la conexión de red entre los dispositivos. Puede configurar la seguridad al configurar la contraseña del nodo RPC seleccionando la casilla de verificación **Proteger**.

Para cambiar la contraseña de un nodo RPC y habilitar una conexión segura

1. Vaya a **Sistema > Red > RPC.**
2. En el panel de detalles, seleccione el nodo y, a continuación, haga clic en **Modificar**.
3. En **Contraseña** y **Confirmar contraseña**, escriba la nueva contraseña.
4. En **Dirección IP de origen**, escriba la dirección IP del sistema del otro dispositivo NetScaler Gateway.
5. Haga clic en **Seguro** y, a continuación, en **Aceptar**

> **Nota:**
>
> Al habilitar la opción **Seguro**, el dispositivo cifra todas las comunicaciones enviadas desde el nodo a otros nodos RPC, lo que asegura la comunicación RPC.

Para cambiar la contraseña de un nodo RPC mediante la CLI

En la línea de comandos, escriba:

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]

show ns rpcNode
<!--NeedCopy-->
```

Ejemplo:

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>
```



```
<!--NeedCopy-->
```

Configuración de los dispositivos primarios y secundarios para obtener alta disponibilidad

January 26, 2024

Después de cambiar la contraseña del nodo RPC y habilitar la comunicación segura, utilice la utilidad de configuración para configurar los nodos de alta disponibilidad de NetScaler Gateway principal y secundario.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Estado de alta disponibilidad, haga clic en Habilitado (participar activamente en HA) y, a continuación, haga clic en Aceptar.

Configuración de intervalos de comunicación

January 26, 2024

Al configurar NetScaler Gateway como un par de alta disponibilidad, puede configurar el NetScaler Gateway secundario para que escuche a intervalos específicos, medidos en milisegundos (mseg). Estos intervalos se conocen como intervalos de saludo e intervalos muertos.

El intervalo de saludo es el intervalo en el que se envían los mensajes de latidos al nodo del mismo nivel. El intervalo muerto es el intervalo de tiempo tras el cual el nodo del par se marca como DOWN si no se reciben paquetes de latidos. Los mensajes de latido son paquetes UDP enviados al puerto 3003 del otro nodo en un par de alta disponibilidad.

Cuando configuras el intervalo de saludo, puede usar los valores 200 a 1000. El valor por defecto es 200. Los valores de intervalo muerto son de 3 a 60. El valor por defecto es 3.

> **Nota**
>
> El intervalo muerto debe establecerse como múltiplo del intervalo de saludo.

Para configurar los intervalos de comunicación para el NetScaler Gateway secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Intervalos, realice una o ambas de las acciones siguientes:
    - En Intervalo de saludo (msec), escriba el valor y, a continuación, haga clic en Aceptar. El valor predeterminado es 200 milisegundos.
    - En Intervalo muerto (segundos), escriba el valor y, a continuación, haga clic en Aceptar. El valor predeterminado es de tres segundos.

Sincronizar dispositivos NetScaler Gateway

January 26, 2024

La sincronización automática de los dispositivos NetScaler Gateway en un par de alta disponibilidad está habilitada de forma predeterminada. Con la sincronización automática, puede realizar cambios en un dispositivo y permitir que los cambios se propaguen automáticamente al segundo dispositivo. La sincronización utiliza el puerto 3010.

La sincronización se inicia cuando ocurre lo siguiente:

- El nodo secundario se reinicia.
- El nodo principal pasa a ser secundario tras una conmutación por error.

Puede inhabilitar la sincronización, lo que impide que NetScaler Gateway secundario sincronice su configuración con la puerta de enlace principal cuando se produce un cambio en el dispositivo principal. También puede forzar la sincronización.

Habilita o inhabilita la sincronización de alta disponibilidad en el nodo secundario del par.

Para habilitar o inhabilitar la sincronización de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En el cuadro de diálogo Configurar nodo, en Sincronización de alta disponibilidad, realice una de las siguientes acciones:

- Para inhabilitar la sincronización, desactive la casilla de verificación El nodo secundario buscará la configuración de Principal.
- Para habilitar la sincronización, seleccione la casilla de verificación Nodo secundario obtendrá la configuración del nodo principal.

4. Haga clic en Aceptar. Aparece un mensaje en la barra de estado que indica que la configuración del nodo se ha realizado correctamente.

Para forzar la sincronización entre dispositivos

Además de la sincronización automática, NetScaler Gateway admite la sincronización forzada entre los dos nodos en un par de alta disponibilidad.

Puede forzar la sincronización en los dispositivos NetScaler Gateway principal y secundario. Sin embargo, si la sincronización ya está en curso, el comando falla y NetScaler Gateway muestra una advertencia. La sincronización forzada también falla en las siguientes circunstancias:

- La sincronización se fuerza en un sistema independiente.
- El nodo secundario está inhabilitado.
- Inhabilitar la sincronización de alta disponibilidad en el nodo secundario.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Nodos, haga clic en Forzar sincronización.

Sincronización de archivos de configuración en una configuración de alta disponibilidad

January 26, 2024

En una configuración de alta disponibilidad, puede sincronizar varios archivos de configuración del nodo principal al nodo secundario.

Parámetros para sincronizar archivos en una configuración de alta disponibilidad

- Modo

  Tipo de sincronización que se va a realizar. Las descripciones siguientes incluyen, entre paréntesis, el argumento de línea de comandos que especifica la opción.

- **Todo excepto licencias y rc.conf** (todo). Sincroniza archivos relacionados con la configuración del sistema, marcadores de NetScaler Gateway, certificados SSL, listas de CRL SSL, scripts de inyección HTML y objetos XML de Application Firewall.
- **Marcadores** (marcadores). Sincroniza todos los marcadores de NetScaler Gateway.
- **Certificados y claves SSL** (`ssl`). Sincroniza todos los certificados, claves y CRL de la función SSL.
- **Licencias y rc.conf** (misc). Sincroniza todos los archivos de licencia y el archivo rc.conf.
- **Todo, incluidas las licencias y rc.conf** (all_plus_misc). Sincroniza archivos relacionados con la configuración del sistema, marcadores de NetScaler Gateway, certificados SSL, listas de CRL SSL, scripts de inyección HTML, objetos XML de Application Firewall, licencias y el archivo rc.conf.

Nota: Hay más opciones disponibles si instala una licencia NetScaler en el dispositivo.

Para sincronizar archivos en una configuración de alta disponibilidad mediante la utilidad de configuración

1. En el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Diagnóstico**.
2. En el panel de detalles, en **Utilidades**, haga clic en **Iniciar sincronización de archivos HA**.
3. En el cuadro de diálogo **Iniciar sincronización de archivos**, en el menú **Modo**, seleccione el tipo de sincronización adecuado (por ejemplo, Todo excepto licencias y rc.conf) y, a continuación, haga clic en **Aceptar**.

Configuración de la propagación de comandos

March 27, 2024

En una configuración de alta disponibilidad, cualquier comando emitido en el nodo principal se propaga automáticamente al nodo secundario y se ejecuta en él antes de que se ejecute el comando en el nodo principal. Si se produce un error en la propagación del comando o si se produce un error en la ejecución del comando en el nodo secundario, el nodo principal ejecuta el comando y registra un error. La propagación de comandos utiliza el puerto 3011.

En una configuración de pares de alta disponibilidad, la propagación de comandos está habilitada de forma predeterminada tanto en el nodo principal como en el secundario. Puede habilitar o inhabilitar la propagación de comandos en cualquiera de los nodos en un par de alta disponibilidad. Si inhabilita la propagación de comandos en el nodo principal, los comandos no se propagan al nodo secundario. Si inhabilita la propagación de comandos en el nodo secundario, los comandos propagados desde el principal no se ejecutan en el nodo secundario.

Nota: Después de volver a habilitar la propagación, recuerde forzar la sincronización.

Nota: Si se produce la sincronización mientras se inhabilita la propagación, los cambios relacionados con la configuración que se realicen antes de que surta efecto la desactivación de la propagación se sincronizarán con el nodo secundario. Esto también es cierto para los casos en los que la propagación está inhabilitada mientras la sincronización está en curso.

Para habilitar o inhabilitar la propagación en el nodo principal

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Alta disponibilidad**.
2. En el panel de detalles, en la pestaña **Nodos** , seleccione un nodo y, a continuación, haga clic en **Editar** .
3. En **Propagación de HA**, realice una de las siguientes acciones:
    - Para inhabilitar la propagación de alta disponibilidad, desactive la casilla de verificación **Nodo principal propaga la configuración secundaria**.
    - Para habilitar la propagación de alta disponibilidad, active la casilla de verificación **Nodo principal propaga la configuración secundaria**.
4. Haga clic en **Aceptar**.

Solución de problemas de propagación de comandos

January 26, 2024

En la lista siguiente se describen los motivos por los que la propagación de comandos puede fallar y las soluciones para restaurar la configuración:

- La conectividad de red no está activa. Si se produce un error en la propagación de un comando, compruebe la conexión de red entre los dispositivos NetScaler Gateway principal y secundario.
- Faltan recursos en NetScaler Gateway secundario. Si la ejecución de un comando se ejecuta correctamente en el NetScaler Gateway principal pero no se propaga al NetScaler Gateway secundario, ejecute el comando directamente en el NetScaler Gateway secundario para ver el mensaje de error. Es posible que el error se haya producido porque los recursos requeridos por el comando están presentes en el NetScaler Gateway principal y no están disponibles en el NetScaler Gateway secundario. Además, compruebe que los archivos de licencia de cada dispositivo coinciden.

Por ejemplo, compruebe que todos los certificados de Secure Sockets Layer (SSL) estén presentes en cada NetScaler Gateway. Compruebe que exista cualquier personalización del script de inicialización en ambos dispositivos NetScaler Gateway.

- Error de autenticación. Si recibe un mensaje de error de error de autenticación, compruebe la configuración del nodo RPC de cada dispositivo.

Configurar el modo a prueba de fallos

January 26, 2024

En una configuración de alta disponibilidad, el modo a prueba de fallos garantiza que un nodo sea siempre principal cuando ambos nodos no superen la comprobación de estado. El modo a prueba de fallos garantiza que cuando un nodo solo está disponible parcialmente, los métodos de copia de seguridad se pueden activar y manejar el tráfico.

El modo a prueba de fallos de alta disponibilidad se configura de forma independiente en cada nodo.

En la tabla siguiente se muestran algunos de los casos a prueba de fallos. El estado NOT_UP significa que el nodo no ha superado la comprobación de estado y, sin embargo, el nodo está parcialmente disponible. El estado UP significa que el nodo ha superado la comprobación de estado.

Tabla 1. Fundas de modo a prueba de fallos

Estado de salud del nodo A (primario)	Estado de salud del nodo B (secundario)	Comportamiento de alta disponibilidad predeterminado	Comportamiento de alta disponibilidad habilitado a prueba de errores	Descripción
NOT_UP (último error)	NOT_UP (error primero)	A (secundaria), B (secundaria)	A (primaria), B (secundaria)	Si ambos nodos fallan, uno tras otro, el nodo que fue el último nodo principal sigue siendo el principal.

Estado de salud del nodo A (primario)	Estado de salud del nodo B (secundario)	Comportamiento de alta disponibilidad predeterminado	Comportamiento de alta disponibilidad habilitado a prueba de errores	Descripción
NOT_UP (error primero)	NOT_UP (último error)	A (secundaria), B (secundaria)	A (secundaria), B (primaria)	Si ambos nodos fallan, uno tras otro, el nodo que fue el último nodo principal sigue siendo el principal.
UP	UP	A (primaria), B (secundaria)	A (primaria), B (secundaria)	Si ambos nodos pasan la comprobación de estado, no hay cambios en el comportamiento con la seguridad contra fallos habilitada.
UP	NOT_UP	A (primaria), B (secundaria)	A (primaria), B (secundaria)	Si solo falla el nodo secundario, no hay cambios en el comportamiento con la opción a prueba de fallos habilitada.
NOT_UP	UP	A (secundaria), B (primaria)	A (secundaria), B (primaria)	Si solo falla el primario, no hay cambios en el comportamiento con la seguridad habilitada.

Estado de salud del nodo A (primario)	Estado de salud del nodo B (secundario)	Comportamiento de alta disponibilidad predeterminado	Comportamiento de alta disponibilidad habilitado a prueba de errores	Descripción
NOT_UP	UP (STAYSEC-ONDARY)	A (secundaria), B (secundaria)	A (primaria), B (secundaria)	Si el secundario está configurado como STAYSECONDARY, el primario sigue siendo primario aunque falle.

Para configurar el modo a prueba de fallos

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En el cuadro de diálogo Configurar nodo, en Modo a prueba de fallos, seleccione Mantener un nodo principal aunque ambos nodos no estén en buen estado y, a continuación, haga clic en Aceptar.

Configuración de la dirección MAC virtual

January 26, 2024

La dirección MAC virtual la comparten los dispositivos NetScaler Gateway principal y secundario en una configuración de alta disponibilidad.

En una configuración de alta disponibilidad, el NetScaler Gateway principal posee todas las direcciones IP flotantes, como la dirección IP asignada o la dirección IP virtual. Responde a las solicitudes de protocolo de resolución de direcciones (ARP) de estas direcciones IP con su propia dirección MAC. Como resultado, la tabla ARP de un dispositivo externo (como un router) se actualiza con la dirección IP flotante y la dirección MAC principal de NetScaler Gateway. Cuando se produce una conmutación por error, el NetScaler Gateway secundario se hace cargo del nuevo NetScaler Gateway principal. A continuación, utiliza el protocolo de resolución de direcciones gratuito (GARP) para anunciar las di-

recciones IP flotantes que adquirió del dispositivo principal. La dirección MAC, que anuncia el nuevo dispositivo principal, es la de su propia interfaz.

Algunos dispositivos no aceptan mensajes GARP generados por NetScaler Gateway. Como resultado, algunos de los dispositivos externos conservan la antigua asignación de IP a Mac anunciada por el antiguo NetScaler Gateway principal. Esta situación puede provocar que un sitio no esté disponible. Para resolver el problema, configure una dirección MAC virtual en ambos dispositivos NetScaler Gateway de un par de alta disponibilidad. Esta configuración implica que ambos dispositivos NetScaler Gateway tienen direcciones MAC idénticas. Como resultado, cuando se produce una conmutación por error, la dirección MAC del NetScaler Gateway secundario permanece sin cambios y no es necesario actualizar las tablas ARP de los dispositivos externos.

Para crear una dirección MAC virtual, cree un identificador de enrutador virtual (ID) y vincúlelo a una interfaz. En una configuración de alta disponibilidad, el usuario debe enlazar el ID a las interfaces de ambos dispositivos.

Cuando el ID del router virtual está enlazado a una interfaz, el sistema genera una dirección MAC virtual con el ID del router virtual como último octeto. Un ejemplo de la dirección MAC virtual genérica es 00:00:5 e: 00:01:\ <VRID\ >. Por ejemplo, si ha creado un ID de enrutador virtual con el valor 60 y lo vincula a una interfaz, la dirección MAC virtual resultante es 00:00:5 e: 00:01:3 c, donde 3c es la representación hexadecimal del ID del router virtual. Puede crear 255 ID de enrutador virtual que van del 1 al 254.

Puede configurar direcciones MAC virtuales para IPv4 e IPv6.

Configurar direcciones MAC virtuales IPv4

January 26, 2024

Cuando crea una dirección MAC virtual IPv4 y la vincula a una interfaz, cualquier paquete IPv4 enviado desde la interfaz utiliza la dirección MAC virtual enlazada a la interfaz. Si no hay ninguna dirección MAC virtual IPv4 enlazada a una interfaz, se utiliza la dirección MAC física de la interfaz.

La dirección MAC virtual genérica tiene el formato 00:00:5 e: 00:01:\ <VRID\ >. Por ejemplo, si crea un VRID con un valor de 60 y lo vincula a una interfaz, la dirección MAC virtual resultante es 00:00:5 e: 00:01:3 c, donde 3c es la representación hexadecimal del VRID. Puede crear 255 VRID con valores del 1 al 255.

Creación o modificación de una dirección MAC virtual IPv4

March 27, 2024

Cree una dirección MAC virtual IPv4 asignándole un ID de enrutador virtual. A continuación, puede enlazar la dirección MAC virtual a una interfaz. No se pueden enlazar varios ID de enrutador virtual a la misma interfaz. Para verificar la configuración de la dirección MAC virtual, debe mostrar y examinar la dirección MAC virtual y las interfaces enlazadas a la dirección MAC virtual.

Parámetros para configurar una dirección MAC virtual

- vRID

  ID del router virtual que identifica la dirección MAC virtual. Valores posibles: 1-255.

- `ifnum`

  El número de interfaz (notación de ranura/puerto) que se va a enlazar a la dirección MAC virtual.

Para configurar una dirección MAC virtual

1. Vaya a **Sistema > Red** y, a continuación, haga clic en **VMAC**.
2. En el panel de detalles, en la ficha **VMAC**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear VMAC**, en **ID de enrutador virtual**, escriba el valor.
4. En **Interfaces asociadas**, en **Interfaces disponibles**, seleccione una interfaz de red, haga clic en **Agregar**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Después de crear la dirección MAC virtual, aparece en la utilidad de configuración. Si ha seleccionado una interfaz de red, el ID del router virtual está enlazado a esa interfaz.

Para eliminar una dirección MAC virtual

Para eliminar una dirección MAC virtual, debe eliminar el ID del router virtual correspondiente.

1. Vaya a **Sistema > Red y,** a continuación, haga clic en **VMAC**.
2. En el panel de detalles, seleccione un elemento y, a continuación, haga clic en **Eliminar**.

Para enlazar y desvincular una dirección MAC virtual

Al crear el ID del enrutador virtual, seleccionó una interfaz de red en NetScaler Gateway y, a continuación, enlazó el ID del router virtual a la interfaz de red. También puede desvincular una dirección MAC virtual de la interfaz de red, pero dejar la dirección MAC configurada en NetScaler Gateway.

1. Vaya a **Sistema > Red** y, a continuación, haga clic en **VMAC**.
2. En el panel de detalles, seleccione un elemento y, a continuación, haga clic en **Abrir**.
3. En **Interfaces configuradas**, seleccione una interfaz de red, haga clic en **Quitar**, en **Aceptar** y, a continuación, en **Cerrar**.

Configurar direcciones MAC virtuales IPv6

January 26, 2024

NetScaler Gateway admite direcciones MAC virtuales para paquetes IPv6. Puede enlazar cualquier interfaz a una dirección MAC virtual para IPv6, incluso si una dirección MAC virtual IPv4 está enlazada a la interfaz. Cualquier paquete IPv6 enviado desde la interfaz utiliza la dirección MAC virtual enlazada a esa interfaz. Si no hay una dirección MAC virtual enlazada a una interfaz, un paquete IPv6 utiliza la MAC física.

Creación o modificación de una dirección MAC virtual para IPv6

January 26, 2024

Cree una dirección MAC virtual IPv6 asignándole un ID de enrutador virtual IPv6. A continuación, vincule la dirección MAC virtual a una interfaz. No se pueden enlazar varios ID de enrutador virtual IPv6 a una interfaz. Para verificar la configuración de la dirección MAC virtual, muestre y examine las direcciones MAC virtuales y las interfaces enlazadas a la dirección MAC virtual.

Parámetros para configurar una dirección MAC virtual para IPv6

- `Virtual Router ID`

  ID del router virtual que identifica la dirección MAC virtual. Valores posibles: 1-255.

- `ifnum`

  El número de interfaz (notación de ranura/puerto) que se va a enlazar a la dirección MAC virtual.

Para configurar una dirección MAC virtual para IPv6

1. En la utilidad de configuración, en la ficha Configuración, expanda **Sistema > Red** y, a continuación, haga clic en VMAC.

2. En el panel de detalles, en la ficha VMAC6, realice una de las siguientes acciones:
    - Para crear una nueva dirección MAC virtual, haga clic en Agregar.
    - Para modificar una dirección MAC virtual existente, haga clic en Abrir.
3. En el cuadro de diálogo Crear VMAC6 o Configurar VMAC6, en ID de enrutador virtual, introduzca el valor, como vRID6.
4. En Asociar interfaces, haga clic en **Agregar > Crear > Cerrar**. Aparece un mensaje en la barra de estado que indica que la dirección MAC virtual está configurada.

Para quitar una dirección MAC virtual para IPv6

1. En la utilidad de configuración, en la ficha Configuración, expanda **Sistema > Red** y, a continuación, haga clic en VMAC.
2. En el panel de detalles, en la ficha VMAC6, seleccione el ID del router virtual que quiere quitar y, a continuación, haga clic en Quitar. Aparece un mensaje en la barra de estado que indica que se ha eliminado la dirección MAC virtual.

Configuración de pares de alta disponibilidad en distintas subredes

January 26, 2024

Una implementación típica de alta disponibilidad es cuando ambos dispositivos de un par de alta disponibilidad residen en la misma subred. Una implementación de alta disponibilidad también puede consistir en dos dispositivos NetScaler Gateway en los que cada dispositivo se encuentra en una red diferente. En este tema se describe esta última configuración e incluye configuraciones de ejemplo y una lista de diferencias entre las configuraciones de alta disponibilidad dentro de una red y entre redes.

También puede configurar la redundancia de enlaces y los monitores de ruta. Estas funciones de NetScaler Gateway resultan útiles en una configuración de alta disponibilidad entre redes. Las funciones también cubren el proceso de comprobación de estado utilizado por cada NetScaler Gateway para garantizar que el dispositivo asociado esté activo.

Cómo funciona la configuración de red independiente

Los dispositivos NetScaler Gateway están conectados a distintos routers, denominados R3 y R4, en dos redes diferentes. Los dispositivos intercambian paquetes de latidos a través de estos routers. Un paquete de latidos es una señal que se produce a intervalos regulares que garantiza que la conexión

siga activa. Puede ampliar esta configuración para dar cabida a implementaciones que impliquen cualquier número de interfaces.

Nota: Si utiliza redirección estática en su red, debe agregar rutas estáticas entre todos los sistemas para asegurarse de que los paquetes de latidos se envían y reciben correctamente. (Si utiliza redirección dinámica en sus sistemas, las rutas estáticas son innecesarias).

Cuando los dispositivos de un par de alta disponibilidad residen en dos redes distintas, el NetScaler Gateway secundario debe tener una configuración de red independiente. Esto significa que los dispositivos NetScaler Gateway de distintas redes no pueden compartir direcciones IP asignadas, LAN virtuales ni rutas de red. Este tipo de configuración, en la que los dispositivos NetScaler Gateway de un par de alta disponibilidad tienen parámetros configurables diferentes, se conoce como configuración de red independiente o configuración de red simétrica.

En la tabla siguiente se resumen los parámetros configurables de una configuración de red independiente y se muestra cómo debe configurarlos en cada NetScaler Gateway:

Parámetros configurables	Comportamiento
Direcciones IP	Específico de NetScaler Gateway Activa solo en ese dispositivo.
Dirección IP virtual	flotante.
LAN virtual	Específico de NetScaler Gateway Activa solo en ese dispositivo.
Rutas	Específico de NetScaler Gateway Activa solo en ese dispositivo. Una ruta de equilibrio de carga de enlace (LLB) es flotante.
listas de control de acceso (ACL)	Flotante (común). Activo en ambos dispositivos.
Redirección dinámica	Específico de NetScaler Gateway Activa solo en ese dispositivo. El NetScaler Gateway secundario también debe ejecutar los protocolos de redirección e intercalar con los enrutadores ascendentes.
Modo L2	Flotante (común). Activo en ambos dispositivos.
Modo L3	Flotante (común). Activo en ambos dispositivos.
Traducción inversa de direcciones de red (NAT)	Específico de NetScaler Gateway Invertir NAT con una dirección IP virtual porque la dirección IP NAT es flotante.

> **Nota:**
>
> IPSET en modo INC es compatible con direcciones IP públicas. Para obtener más información, consulte Diseño de referencia validado de IP front-end de NetScaler High Availability with Azure Load Balancer.

Agregar un nodo remoto

January 26, 2024

Cuando dos nodos de un par de alta disponibilidad residen en subredes distintas, cada nodo debe tener una configuración de red diferente. Por lo tanto, para configurar dos sistemas independientes para que funcionen como un par de alta disponibilidad, debe especificar el modo de cómputo de red independiente durante el proceso de configuración.

Cuando agrega un nodo de alta disponibilidad, debe inhabilitar el monitor de alta disponibilidad para cada interfaz que no esté conectada o que se esté usando para el tráfico.

Para agregar un nodo remoto para el modo de cómputo de red independiente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, haga clic en la ficha **Nodos** y, a continuación, haga clic en **Agregar**.
3. En el cuadro de diálogo Configuración de alta disponibilidad, en el cuadro de texto **Dirección IP del nodo remoto**, escriba la dirección IP de NetScaler Gateway del dispositivo que es el nodo remoto.

   Para utilizar una dirección IPv6, haga clic en la casilla de verificación **IPv6** antes de introducir la dirección IP.
4. Si quiere agregar el nodo local al nodo remoto automáticamente, seleccione Configurar sistema remoto para participar en la configuración de alta disponibilidad. Si no selecciona esta opción, debe iniciar sesión en el dispositivo representado por el nodo remoto y agregar el nodo que está configurando actualmente.
5. Haga clic para habilitar el monitor de alta disponibilidad claro en las interfaces/canales que están inactivos.
6. Haga clic para activar el modo Activar el modo INC (Configuración de red independiente) en modo automático.

7. Haga clic en **Aceptar**. La página **Nodos** muestra los nodos locales y remotos de la configuración de alta disponibilidad.

Para quitar un nodo remoto

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **Sistema > Alta disponibilidad**.
2. En el panel de detalles, haga clic en la ficha **Nodos**.
3. Seleccione el nodo que quiere quitar, haga clic en Quitar y **, a continuación,** haga clic en **Sí**.

Configuración de monitores de rutas

January 26, 2024

Puede utilizar monitores de rutas para hacer que el estado de alta disponibilidad dependa de la tabla de redirección interna, independientemente de si la tabla contiene rutas estáticas o aprendidas dinámicamente. En una configuración de alta disponibilidad, un monitor de ruta en cada nodo comprueba la tabla de redirección interna para asegurarse de que siempre haya una entrada de ruta para llegar a una red concreta. Si la entrada de ruta no está presente, el estado del monitor de ruta cambia a DOWN.

Cuando un dispositivo NetScaler Gateway solo tiene rutas estáticas para llegar a una red y quiere crear un monitor de rutas para la red, debe habilitar las rutas estáticas supervisadas para las rutas estáticas. La ruta estática supervisada elimina las rutas estáticas inalcanzables de la tabla de redirección interna. Si inhabilita rutas estáticas supervisadas en rutas estáticas, una ruta estática inalcanzable puede permanecer en la tabla de redirección interno, lo que contradice el propósito de tener el monitor de ruta.

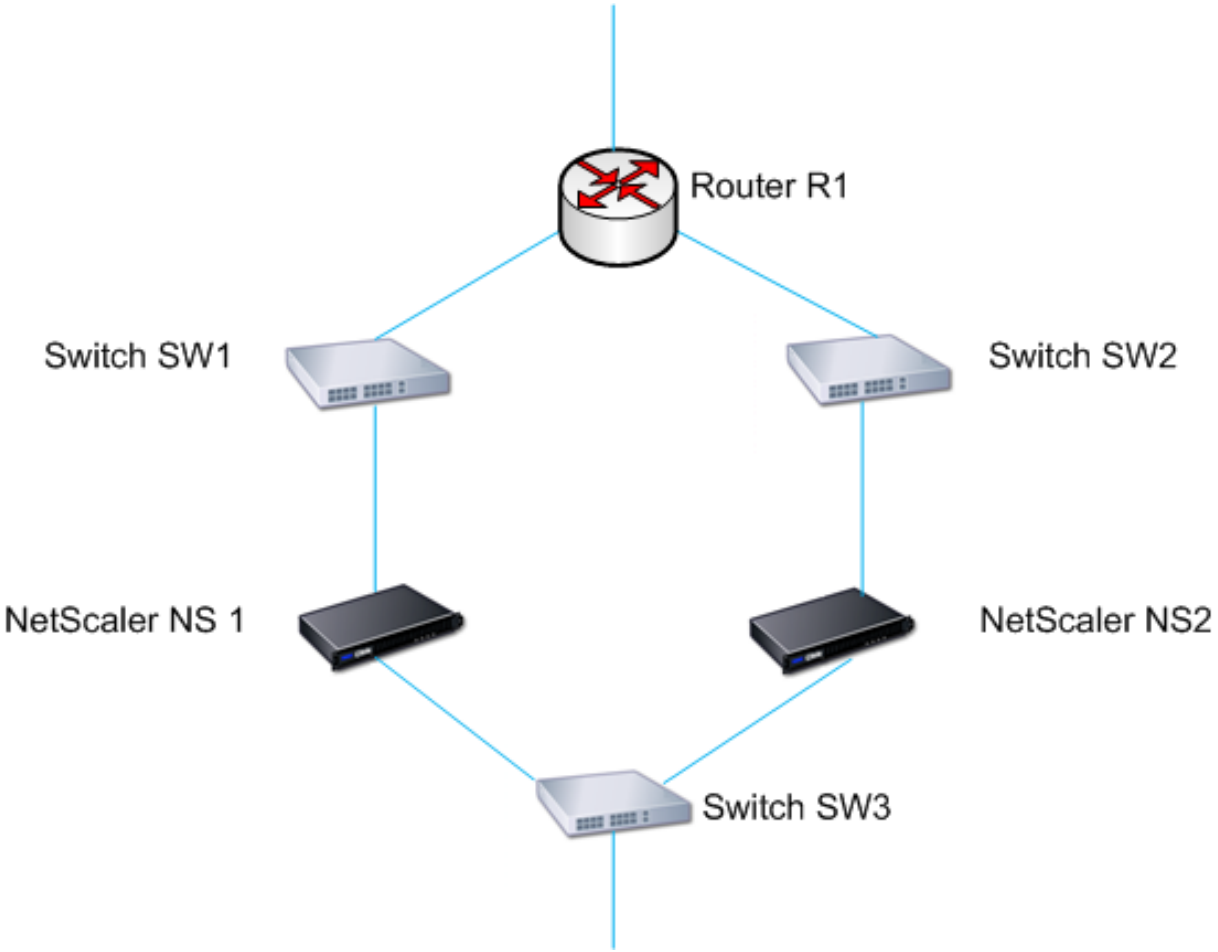
Los monitores de ruta son compatibles con la configuración de red independiente habilitada o inhabilitada. La tabla siguiente muestra lo que ocurre con los monitores de ruta en una configuración de alta disponibilidad y con Configuración de red independiente habilitada o inhabilitada.

Monitores de ruta en alta disponibilidad en el modo de configuración de red independiente inhabilitado	Monitores de ruta en alta disponibilidad en el modo Configuración de red independiente habilitado
Los monitores de ruta se propagan por nodos y se intercambian durante la sincronización.	Los monitores de ruta no se propagan por los nodos ni se intercambian durante la sincronización.

Monitores de ruta en alta disponibilidad en el modo de configuración de red independiente inhabilitado	Monitores de ruta en alta disponibilidad en el modo Configuración de red independiente habilitado
Los monitores de ruta solo están activos en el nodo principal actual. El dispositivo NetScaler Gateway siempre muestra el estado de un monitor de ruta como UP, independientemente de si la entrada de ruta está presente o no en la tabla de redirección interna. Un monitor de ruta comienza a supervisar su ruta en los siguientes casos, para permitir que NetScaler Gateway aprenda las rutas dinámicas, lo que puede tardar hasta 180 segundos: reinicio, conmutación por error, comando set route6 para rutas v6, comando set route `msr` enable/disable para rutas v4, agregar un nuevo monitor de ruta	Los monitores de ruta están activos tanto en el nodo principal como en el secundario. El dispositivo NetScaler Gateway muestra el estado del monitor de ruta como DOWN si la entrada de ruta correspondiente no está presente en la tabla de redirección interna. No aplicable.

Los monitores de ruta son útiles cuando inhabilita el modo de configuración de red independiente y quiere que una puerta de enlace de un nodo principal sea inalcanzable como una de las condiciones para la conmutación por error de alta disponibilidad.

Por ejemplo, inhabilita la Configuración de red independiente en una configuración de alta disponibilidad en una topología de dos brazos que tiene dispositivos NetScaler Gateway NS1 y NS2 en la misma subred, con el enrutador R1 y los conmutadores SW1, SW2 y SW3, como se muestra en la siguiente ilustración. Dado que R1 es el único enrutador de esta configuración, quiere que la configuración de alta disponibilidad conmute por error siempre que no se pueda acceder a R1 desde el nodo principal actual. Puede configurar un monitor de ruta (por ejemplo, RM1 y RM2, respectivamente) en cada uno de los nodos para supervisar la accesibilidad de R1 desde ese nodo.



Con NS1 como nodo principal actual, el flujo de red es el siguiente:

1. El monitor de ruta RM1 en NS1 monitorea la tabla de redirección interno de NS1 para detectar la presencia de una entrada de ruta para el enrutador R1. NS1 y NS2 intercambian mensajes de latidos a través del switch SW1 o SW3 a intervalos regulares.
2. Si el conmutador SW1 falla, el protocolo de redirección de NS1 detecta que no se puede acceder a R1 y, por lo tanto, elimina la entrada de ruta para R1 de la tabla de redirección interna. NS1 y NS2 intercambian mensajes de latidos a través del switch SW3 a intervalos regulares.
3. Al detectar que la entrada de ruta para R1 no está presente en la tabla de redirección interno, RM1 inicia una conmutación por error. Si la ruta a R1 está inactiva desde NS1 y NS2, la conmutación por error se produce cada 180 segundos hasta que uno de los dispositivos puede llegar a R1 y restaurar la conexión.

Agregar o quitar monitores de ruta

January 26, 2024

Cuando los dispositivos de un par de alta disponibilidad residen en redes diferentes, el estado de alta disponibilidad de NetScaler Gateway depende de si se puede acceder al dispositivo o no. En una configuración de alta disponibilidad entre redes, un monitor de ruta de cada NetScaler Gateway explora la tabla de redirección interna para asegurarse de que siempre haya una entrada para el otro NetScaler Gateway.

Para agregar un monitor de ruta

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el cuadro de diálogo Enlazar/desenlazar monitores de ruta, en la ficha Supervisores de ruta, haga clic en Acción y, a continuación, en Configurar.
3. En Especificar monitor de ruta, en Red, escriba la dirección IP de la red del otro dispositivo NetScaler Gateway.

   Para configurar una dirección IPv6, haga clic en IPv6 y, a continuación, escriba la dirección IP.
4. En Máscara de red, escriba la máscara de subred de la otra red, haga clic en Agregar y, a continuación, haga clic en Aceptar.

Cuando se complete este procedimiento, el monitor de ruta se enlazará a NetScaler Gateway.

Nota: Cuando un monitor de ruta no está vinculado a un NetScaler Gateway, el estado de alta disponibilidad de cualquiera de los dispositivos viene determinado por el estado de las interfaces.

Para quitar un monitor de ruta

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Supervisores de ruta, haga clic en Acción y, a continuación, en Configurar.
3. En Monitores de ruta configurados, seleccione el monitor, haga clic en Eliminar y, a continuación, haga clic en Aceptar.

Configuración de redundancia de enlaces

January 26, 2024

La redundancia de vínculos agrupa las interfaces de red para evitar la conmutación por error debido a un error en una interfaz de red de un NetScaler Gateway que tiene otras interfaces en funcionamiento.

El error de la primera interfaz del NetScaler Gateway principal desencadena la conmutación por error, aunque la primera interfaz puede seguir usando su segundo enlace para atender las solicitudes de los usuarios. Al configurar la redundancia de vínculos, puede agrupar las dos interfaces en un conjunto de interfaces de conmutación por error, lo que evita que el error de un solo enlace provoque la conmutación por error al NetScaler Gateway secundario, a menos que todas las interfaces del NetScaler Gateway principal no funcionen.

Cada interfaz de un conjunto de interfaces de conmutación por error mantiene entradas de puente independientes. Las interfaces de supervisión habilitadas y de alta disponibilidad en un NetScaler Gateway que no están vinculadas a un conjunto de interfaces con errores se conocen como interfaces críticas, porque si alguna de estas interfaces falla, se desencadena la conmutación por error.

Para configurar la redundancia de enlaces

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, haga clic en Agregar.
3. En Nombre, escriba un nombre para el conjunto.
4. En Interfaces, haga clic en Agregar.
5. En Interfaces disponibles, seleccione una interfaz y, a continuación, haga clic en la flecha para mover la interfaz a Configurada.
6. Repita los pasos 4 y 5 para la segunda interfaz y, a continuación, haga clic en Crear.

Puede agregar tantas interfaces como necesite para la conmutación por error entre las interfaces.

Para quitar interfaces del conjunto de interfaces de conmutación por error

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, seleccione un conjunto y, a continuación, haga clic en Quitar.

Para quitar un conjunto de interfaces de conmutación por error

Si ya no necesita un conjunto de interfaces de conmutación por error, puede quitarlo de NetScaler Gateway.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En la ficha Conjunto de interfaces de conmutación por error, seleccione un conjunto y, a continuación, haga clic en Quitar.

Descripción de las causas de la conmutación por error

January 26, 2024

Los siguientes eventos pueden provocar una conmutación por error en una configuración de alta disponibilidad:

1. Si el nodo secundario no recibe un paquete de latidos del nodo principal durante un período de tiempo que exceda el intervalo muerto establecido en el secundario. Para obtener más información sobre cómo establecer el intervalo muerto, consulte Configuración de intervalos de comunicación. Entre las posibles causas de que un nodo no reciba paquetes de latidos de un nodo del mismo nivel se incluyen:
    - Un problema de configuración de red impide que los latidos recorran la red entre los nodos de alta disponibilidad.
    - El nodo del mismo nivel experimenta un error de hardware o software que hace que se congele (cuelgue), se reinicie o detenga el procesamiento y el reenvío de paquetes de latidos.
2. El nodo principal experimenta un fallo de hardware en su tarjeta SSL.
3. El nodo principal no recibe paquetes de latidos en sus interfaces de red durante tres segundos.
4. En el nodo principal, se produce un error en una interfaz de red que no forma parte de un conjunto de interfaces de conmutación por error (FIS) ni de un canal de agregación de enlaces (LA) y que tiene habilitado el monitor de alta disponibilidad (HAMON). Las interfaces están habilitadas, pero pasan al estado DOWN.
5. En el nodo principal, todas las interfaces de un FIS fallan. Las interfaces están habilitadas, pero pasan al estado DOWN.
6. En el nodo principal, falla un canal LA con HAMON habilitado. Las interfaces están habilitadas, pero pasan al estado DOWN.
7. En el nodo principal, todas las interfaces fallan. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
8. En el nodo principal, todas las interfaces se inhabilitan manualmente. En este caso, la conmutación por error se produce independientemente de la configuración de HAMON.
9. Para forzar una conmutación por error, se ejecuta el comando forzar conmutación por error en cualquiera de los nodos.
10. Un monitor de ruta enlazado al nodo principal se desactiva.

Forzar la conmutación por error desde un nodo

January 26, 2024

Es posible que quiera forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar el nodo principal. Puede forzar la conmutación por error desde el nodo principal o el nodo secundario. Una conmutación por error forzada no se propaga ni sincroniza. Para ver el estado de sincronización tras una conmutación por error forzada, puede ver el estado del nodo.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

- Se fuerza la conmutación por error en un sistema independiente.
- El nodo secundario está inhabilitado.
- El nodo secundario está configurado para permanecer secundario.

El dispositivo NetScaler Gateway muestra un mensaje de advertencia si detecta un problema potencial al ejecutar el comando force failover. El mensaje incluye la información que ha desencadenado la advertencia y solicita confirmación antes de continuar.

Forzar la conmutación por error en el nodo principal o secundario

January 26, 2024

Si fuerza la conmutación por error en el nodo principal, el principal se convierte en el secundario y el secundario en el principal. La conmutación por error forzada solo es posible cuando el nodo principal puede determinar que el nodo secundario está UP.

Si el nodo secundario es DOWN, el comando force failover devuelve el siguiente mensaje de error: "Operation not possible due to invalid peer state. Rectificar y volver a intentarlo."

Si el sistema secundario está en estado de reclamación o inactivo, el comando devuelve el siguiente mensaje de error: `"Operation not possible now. Please wait for system to stabilize before retrying."`

Si ejecuta el comando force failover desde el nodo secundario, el nodo secundario se convierte en primario y el nodo primario se convierte en secundario. Solo se puede producir una conmutación por error forzada si el estado del nodo secundario es correcto y el nodo no está configurado para permanecer secundario.

Si el nodo secundario no puede convertirse en el nodo principal o si el nodo secundario se configuró para permanecer secundario (mediante la opción STAYSECONDARY), el nodo muestra el siguiente mensaje de error: "La operación no es posible porque mi estado no es válido. Vea el nodo para obtener más información. "

Para forzar la conmutación por error en el nodo principal o secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el nodo principal y, a continuación, en Acciones, haga clic en Forzar conmutación por error.
3. En el cuadro de diálogo Advertencia, haga clic en Sí.

Obligar al nodo primario a permanecer primario

January 26, 2024

En una configuración de alta disponibilidad, puede forzar que el NetScaler Gateway principal permanezca como principal incluso después de la conmutación por error del dispositivo. Solo puede configurar esta configuración en dispositivos NetScaler Gateway independientes y en NetScaler Gateway que es el dispositivo principal en un par de alta disponibilidad.

Para forzar que el nodo principal permanezca como principal

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione un nodo y, a continuación, haga clic en Modificar.
3. En Estado de alta disponibilidad, haga clic en Mantente principal y, a continuación, en Aceptar.

Solo puede borrar esta configuración mediante el siguiente comando:

```
clear configuration full
```

Los siguientes comandos no cambian la configuración de alta disponibilidad de NetScaler Gateway:

```
clear configuration basic
```

```
clear configuration extended
```

Obligar al nodo secundario a permanecer secundario

March 27, 2024

En una configuración de alta disponibilidad, puede forzar que el NetScaler Gateway secundario permanezca secundario, independientemente del estado del NetScaler Gateway principal. Cuando configura NetScaler Gateway para que permanezca secundario, sigue siendo secundario aunque se produzca un error en el NetScaler Gateway principal.

Por ejemplo, en una configuración de alta disponibilidad existente, supongamos que necesita actualizar el NetScaler Gateway principal y que este proceso lleva un tiempo determinado. Durante la actualización, el NetScaler Gateway principal puede dejar de estar disponible, pero no quiere que el NetScaler Gateway secundario se haga cargo. Quiere que siga siendo el NetScaler Gateway secundario, incluso si detecta un error en el NetScaler Gateway principal.

Si el estado de un NetScaler Gateway en un par de alta disponibilidad está configurado para permanecer secundario, no participa en las transiciones de máquinas de estado de alta disponibilidad. Puede comprobar el estado de NetScaler Gateway en la utilidad de configuración de la ficha **Nodos**.

Esta configuración funciona tanto en un NetScaler Gateway independiente como en un secundario.

Cuando se establece el nodo de alta disponibilidad, no se propaga ni sincroniza y solo afecta a NetScaler Gateway en el que se configura la configuración.

Para forzar que el nodo secundario permanezca secundario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la pestaña Nodos , seleccione un nodo y, a continuación, haga clic en Editar .
3. En Estado de alta disponibilidad, haga clic en Permanecer en segundo plano (permanecer en modo de escucha) y, a continuación, haga clic en Aceptar.

Para devolver NetScaler Gateway al servicio como dispositivo activo de alta disponibilidad

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Alta disponibilidad.
2. En el panel de detalles, en la ficha Nodos, seleccione el dispositivo que va a seguir siendo el nodo principal y, a continuación, haga clic en Abrir.
3. En Estado de alta disponibilidad, haga clic en Habilitado (participar activamente en HA) y, a continuación, haga clic en Aceptar.

Usar clústeres

January 26, 2024

NetScaler Gateway se puede implementar en configuraciones de clúster para proporcionar un alto rendimiento, alta disponibilidad y escalabilidad para el tráfico de clientes VPN. En un clúster, un grupo de dispositivos o máquinas virtuales de NetScaler Gateway funciona como una única imagen del sistema para coordinar las sesiones de los usuarios y administrar el tráfico a los recursos de red. Un clúster de NetScaler Gateway se puede crear con un mínimo de dos y un máximo de 32 dispositivos NetScaler Gateway o máquinas virtuales configuradas como nodos de clúster.

Lea la documentación de
NetScaler Clustering antes de empezar a configurar el clúster de NetScaler Gateway. Preste especial atención a los siguientes temas de esa documentación.

- Consulte Requisitos de hardware y software para comprobar que los sistemas que piensa utilizar cumplen los requisitos.
- Consulte Cómo funciona la agrupación en clústeres para obtener una descripción de los conceptos de clustering
- Consulte Configuración de la comunicación entre nodos para planificar la implementación e identificar cualquier advertencia que pueda ser relevante para su entorno.

Un clúster de NetScaler Gateway funciona como un clúster NetScaler de tipo de configuración VIP detectado.

> **Importante:**
>
> El asistente de **XenApp y XenDesktop** no es compatible con la creación de clústeres y, por lo tanto, no encontrará el asistente de **XenApp y XenDesktop** en la **GUI > Panel de navegación > Sección Integración con productos de NetScaler** .

Configuración de la agrupación en clústeres

March 27, 2024

Las principales tareas de configuración de clústeres de NetScaler Gateway son:

1. Decida qué dispositivo NetScaler Gateway o máquina virtual es el coordinador de configuración y cree una instancia de clúster en ese sistema (si no hay ninguna).
2. Unir los sistemas NetScaler Gateway al clúster como nodos.

3. Crea un grupo de nodos en la instancia del clúster con la opción STICKY definida.
4. Enlazar un único nodo de clúster al grupo de nodos del clúster.
5. Configure un servidor virtual NetScaler Gateway en el coordinador de configuración y vincúlelo al grupo de nodos del clúster.

Hay varios métodos disponibles para configurar un clúster de NetScaler. El siguiente conjunto de tareas utiliza el método más directo disponible en la utilidad de configuración.

Para crear una instancia de clúster de NetScaler Gateway mediante la utilidad de configuración

Una vez que haya ordenado los detalles de la implementación, comience la configuración en NetScaler Gateway que es el coordinador de configuración.

Precaución: Al crear la instancia de clúster, se borra la configuración. Si necesita guardar la configuración del sistema existente como referencia, archive una copia antes de continuar con la configuración del clúster. Cualquier configuración existente que se vaya a utilizar en el clúster se puede volver a aplicar en el coordinador de configuración una vez establecido el clúster.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección NSIP.
2. Expanda el nodo Sistema y, a continuación, el subnodo Cluster.
3. En el panel de detalles, haga clic en Administrar clúster.
4. En el cuadro de diálogo Configuración del clúster, defina los parámetros necesarios para crear el clúster.

    a) Introduzca un ID de instancia de clúster El ID de instancia de clúster es el identificador numérico de la instancia de clúster. El valor predeterminado es 1 pero se puede establecer en cualquier número del 1 al 16.
    b) Introduzca la dirección IP del clúster. La dirección IP del clúster es la dirección IP del coordinador de configuración del clúster, que es la dirección IP de administración del clúster.
    c) Seleccione la interfaz de plano posterior preferida. Esta es la interfaz de NetScaler Gateway que se utiliza para la comunicación entre los nodos del clúster.

5. Haga clic en Crear.
6. En el mensaje para confirmar el reinicio del sistema, haga clic en Sí.
7. Una vez que el nodo esté activo y la sincronización se haya realizado correctamente, desde la dirección IP del clúster, cambie las credenciales RPC de la dirección IP del nodo y del clúster. Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.
8. Espere a que se reinicie el sistema. Una vez disponible, inicie sesión en la utilidad de configuración en la dirección IP del clúster configurada en el paso 4 (2).

Nota: En el panel de **detalles Información del sistema**, el nodo local de la dirección NSIP se indica como coordinador de configuración. Esto confirma que la instancia del clúster base ya está funcionando.

El nodo local del coordinador de configuración se agrega automáticamente al clúster. Se pueden agregar más nodos en la siguiente tarea.

Agregar nodos a un clúster de NetScaler Gateway

Una vez establecida la instancia del clúster, puede empezar a agregar otros nodos de NetScaler Gateway al clúster.

Para agregar más sistemas NetScaler Gateway al clúster, puede utilizar la utilidad de configuración para emitir de forma remota la configuración cluster-node-creation y join-cluster.

Nota: La adición de nodos al clúster debe completarse antes de configurar la configuración de NetScaler Gateway. De esta forma, no tiene que repetir la configuración de NetScaler Gateway si hay algún problema con la configuración del clúster y quiere quitar el clúster y empezar de nuevo.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección IP del clúster.
2. Expanda el nodo **Sistema** y, a continuación, el subnodo Clúster.
3. En el panel de detalles, haga clic en **Administrar clúster**.
4. En el panel de detalles Nodos de clúster, haga clic en **Agregar**.
5. En el panel **Crear nodo de clúster**, introduzca un identificador de nodo único para este nodo.
6. Introduzca la dirección IP de NetScaler del sistema que quiere agregar como nodo de clúster.
7. En el panel **Credenciales del nodo de clúster**, introduzca el nombre de usuario y la contraseña de NetScaler Gateway para el sistema NetScaler Gateway remoto.
8. En el panel Credenciales del Coordinador de configuración, introduzca la contraseña del usuario autorizado local.
9. Haga clic en **Crear**.
10. Cuando se le solicite, haga clic en **SÍ** para permitir que se guarde la configuración del sistema y realice un reinicio en caliente del NetScaler Gateway remoto.
11. Una vez que el nodo esté activo y la sincronización se haya realizado correctamente, desde la dirección IP del clúster, cambie las credenciales RPC de la dirección IP del nodo y del clúster. Para obtener más información sobre cómo cambiar la contraseña de un nodo RPC, consulte Cambiar una contraseña de nodo RPC.

Repita los pasos 4 a 11 para cada sistema NetScaler Gateway remoto adicional que quiera configurar como nodo de clúster.

Compruebe que los nodos del clúster estén incluidos en la lista de nodos activos del panel de detalles Nodos de clúster. Si falta algún nodo, repita los pasos 4 a 10 hasta que aparezcan todos los nodos necesarios.

Creación de un grupo de nodos de clúster

Una vez agregados los nodos del clúster, se puede crear un grupo de nodos de clúster.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección IP del clúster.
2. Expanda el nodo **Sistema** y, a continuación, el subnodo Clúster.
3. Pulse en **Grupos de nodos**.
4. En el panel de detalles, haga clic en **Agregar**.
5. Introduzca un nombre para el grupo de nodos del clúster.
6. Seleccione la opción **Sticky** para admitir el tipo de servidor virtual de NetScaler Gateway.
7. Haga clic en **Continuar**.

El grupo de nodos del clúster ya está establecido. Antes de abandonar esta área de la utilidad de configuración, puede enlazar el nodo local de NetScaler Gateway al nuevo grupo de nodos del clúster. Este es el único nodo enlazado al grupo de clústeres.

Vincular el nodo del clúster local al grupo de nodos del clúster

Dado que una configuración de clúster de NetScaler Gateway es de tipo detectado, solo se puede enlazar un nodo al grupo de nodos. El siguiente procedimiento vincula el nodo local del coordinador de configuración al grupo de nodos, pero cualquier nodo del clúster se puede utilizar para este enlace.

1. En el panel Opciones avanzadas, expanda Nodos de clúster.
2. En el panel central Nodos de clúster, seleccione Sin nodo de clúster.
3. En la pantalla Configuración del nodo de clúster, haga clic en Vincular.
4. Seleccione el nodo local representado por la dirección NSIP de este sistema NetScaler Gateway.
5. Haga clic en Insertar.
6. Haga clic en Aceptar.
7. Haga clic en Listo.

El clúster ya está lleno y listo para compartir un servidor virtual de NetScaler Gateway según lo configurado mediante la siguiente tarea.

Enlace de un servidor virtual de NetScaler Gateway al grupo de nodos de clú

Con un clúster establecido, puede proceder a crear la configuración de NetScaler Gateway para la que está destinada la implementación del clúster. Para vincular la configuración al clúster, debe crear el servidor virtual de NetScaler Gateway y vincularlo a un grupo de nodos del clúster configurado en el tipo Sticky. Una vez enlazado el servidor virtual al grupo de nodos del clúster, puede seguir configurando NetScaler Gateway.

Si hay varios servidores virtuales de NetScaler Gateway configurados, estos deben estar enlazados también al grupo de nodos del clúster.

Nota: Si los servidores virtuales de NetScaler Gateway aún no se han configurado, es posible que tenga que habilitar primero las funciones de NetScaler Gateway y Autenticación, autorización y auditoría en
Sistema > Configuración > Configurar funciones básicas.

1. Inicie sesión en la utilidad de configuración de NetScaler en la dirección IP del clúster.
2. Expanda el nodo **Sistema** y, a continuación, el subnodo Clúster.
3. Pulse en **Grupos de nodos**.
4. En el panel **Grupo de nodos**, seleccione el nombre del grupo de nodos deseado y, a continuación, haga clic en **Modificar**.
5. En el panel **Avanzadas** de la derecha, expanda la opción **Servidores virtuales** y, a continuación, haga clic en el icono + para agregar un servidor virtual.
6. Elija el tipo de servidor virtual VPN y, a continuación, haga clic en **Continuar**.
7. Haga clic en **Bind**.
8. Si aparece el servidor virtual necesario, selecciónelo, haga clic en **Insertar** y, a continuación, haga clic en **Aceptar**.
9. Si tiene que crear un nuevo servidor virtual, haga clic en **Agregar**. Continúe con la configuración del servidor virtual de NetScaler. Como mínimo, todo lo que se necesita es crear el servidor virtual para que se pueda enlazar al grupo de nodos del clúster.
10. Una vez que el servidor virtual esté disponible en la lista Servidores virtuales de NetScaler Gateway, selecciónelo y, a continuación, haga clic en **Insertar**.
11. Haga clic en **Aceptar**.
12. Haga clic en **Listo**.

Nota: Si hay varios servidores virtuales de NetScaler Gateway configurados, también deben enlazarse al grupo de nodos del clúster mediante el mismo método.

Unified Gateway

January 26, 2024

NetScaler con Unified Gateway: una URL

NetScaler con Unified Gateway permite un acceso seguro y simplificado a cualquier aplicación mediante una única URL para usuarios de escritorio y móviles. Detrás de esta única URL, los administradores tienen un único punto de configuración, seguridad y control del acceso remoto a las apli-

caciones. Además, los usuarios remotos tienen una experiencia mejorada con un inicio de sesión único sin interrupciones en todas las aplicaciones que necesitan, junto con el inicio de sesión/cierre de sesión una vez que son fáciles de usar.

Para lograrlo, NetScaler with Gateway, junto con las capacidades de conmutación de contenido de NetScaler y la amplia infraestructura de autenticación, proporciona acceso a sitios y aplicaciones de la organización a través de esta única URL. Además, los usuarios remotos pueden usar dispositivos móviles iOS o Android y sistemas Linux, PC o Mac con el cliente Citrix Secure Access para acceder de manera uniforme a la URL de Unified Gateway, estén donde estén.

Una implementación de Unified Gateway permite el acceso de una sola URL a las siguientes categorías de aplicaciones:

- Aplicaciones de intranet.
- Aplicaciones sin cliente
- Aplicación Software as a Service
- Aplicaciones preconfiguradas atendidas por NetScaler
- Aplicaciones publicadas de Citrix Virtual Apps and Desktops

Las aplicaciones de intranet pueden ser cualquier aplicación basada en web que resida dentro de la red empresarial segura. Se trata de recursos internos como un sitio de la intranet de la organización, una aplicación de seguimiento de errores o una wiki.

Por lo general, también residen dentro de la red empresarial segura, las **aplicaciones sin cliente** Unified Gateway proporciona acceso a una única URL son Outlook Web Access y SharePoint. Estas aplicaciones proporcionan acceso al correo electrónico de Exchange y a los recursos del equipo sin software cliente dedicado que debe estar disponible para los usuarios remotos.

Las aplicaciones SaaS, también conocidas comúnmente como Cloud Apps, son aplicaciones externas basadas en la nube de las que dependen las organizaciones, como ShareFile, Salesforce o NetSuite. El inicio de sesión único basado en SAML es compatible con las aplicaciones SaaS que lo ofrecen.

Es posible que algunas organizaciones hayan**preconfigurado aplicaciones servidas de NetScaler**implementadas en una configuración de equilibrio de carga de NetScaler. A menudo, esto también se conoce como una aplicación de "proxy inverso". Unified Gateway admite estas aplicaciones cuando un servidor virtual para la implementación reside en la misma instancia o dispositivo de NetScaler Unified Gateway. Estas aplicaciones pueden tener su propia configuración de autenticación que es independiente de la configuración de Unified Gateway.

Todas **las aplicaciones publicadas de Citrix Virtual Apps and Desktops publicadas**pueden estar disponibles a través de una URL de Unified Gateway. Las directivas de SmartAccess y SmartControl pueden aplicarse opcionalmente a directivas granulares y control de acceso a estos recursos.

Asistente de configuración de Unified Gateway

El método recomendado para configurar una implementación de NetScaler con Unified Gateway consiste en utilizar el asistente de configuración de Unified Gateway.El asistente le guía por la configuración y crea todos los servidores virtuales, directivas y expresiones necesarios, y aplica la configuración según los detalles proporcionados. Tras la configuración inicial, el asistente se puede utilizar para administrar la implementación y supervisar su funcionamiento.

> **Nota:**
>
> El asistente de configuración de Unified Gateway no realiza una configuración inicial del sistema. El dispositivo NetScaler Gateway o la instancia VPX deben haber completado la instalación básica antes de configurar Unified Gateway. Consulte las instrucciones de instalación deConfiguración de NetScaler Gateway con el Asistente para configuración inicialpara completar la configuración básica.

Los elementos de Unified Gateway configurados por el asistente son:

- El servidor virtual principal de Unified Gateway
- Certificado de servidor SSL para el servidor virtual de Unified Gateway
- Una configuración de autenticación primaria y otra secundaria opcional
- Selección del tema del portal y personalización opcional
- Las aplicaciones de usuario a las que se debe acceder a través del portal de Unified Gateway

Para cada uno de estos elementos, es necesario proporcionar información de configuración. Para una implementación básica de Unified Gateway, se necesita la siguiente información.

- Para el servidor virtual de Unified Gateway principal, la dirección IP pública y el número de puerto IP de la implementación. Esta es la dirección IP que se resuelve en DNS en el nombre de host de la URL de Unified Gateway. Por ejemplo, si la URL de la implementación de Unified Gateway es `https://mycompany.com/`, la dirección IP debe resolverse en miempresa.com.
- El certificado de servidor SSL firmado para la implementación. NetScaler Gateway admite certificados con formato PEM o PFX.
- Información del servidor de autenticación principal. Los sistemas de autenticación compatibles con esta configuración de autenticación son LDAP/Active Directory, RADIUS y basados en certificados. También se puede crear una configuración de autenticación LDAP o RADIUS secundaria. La dirección IP del servidor de autenticación debe proporcionarse junto con las credenciales de administrador o los atributos de directorio pertinentes. Para la autenticación de certificados, se deben proporcionar los atributos del certificado de dispositivo y un certificado de CA.

- Es posible que se haya seleccionado un tema del portal. Si se quiere un diseño de portal personalizado o con marca, es posible que se carguen gráficos personalizados en el sistema con el asistente.
- Para las aplicaciones de usuario basadas en web, se deben especificar las URL de las aplicaciones individuales. En el caso de las aplicaciones web que van a utilizar la autenticación de inicio de sesión único de SAML, la utilidad recopila la URL de Assertion Consumer Service junto con otros parámetros SAML opcionales. Recopile los detalles de configuración de antemano para las aplicaciones que utilizan un sistema de autenticación SAML.
- Para que los recursos publicados de Citrix Virtual Apps and Desktops estén disponibles a través de la implementación de Unified Gateway, debe especificar el punto de integración (StoreFront, la Interfaz Web o la Interfaz Web en NetScaler). La utilidad requiere el nombre de dominio completo del punto de integración, la ruta del sitio, el dominio de inicio de sesión único, la URL del servidor de Secure Ticket Authority (STA) y otros, según el tipo de punto de integración.

Administración de configuración adicional

Para la configuración específica del sitio que no está disponible en la utilidad de configuración de Unified Gateway, como configuraciones SSL alternativas o directivas de sesión, puede administrar la configuración necesaria en la utilidad de configuración de NetScaler Gateway. Puede modificar esta configuración en los servidores virtuales de Content Switching o VPN una vez creada por la utilidad de configuración de Unified Gateway.

Servidor virtual de cambio de contenido

Se trata de la entidad de configuración de NetScaler detrás de la dirección IP y la URL principales de la implementación. Los certificados y parámetros del servidor SSL se administran en este servidor virtual. Dado que este servidor virtual es el host de red que responde a la implementación, la respuesta del servidor ICMP y el estado de RHI se pueden modificar en este servidor virtual, si es necesario. El servidor virtual de conmutación de contenido se encuentra en la ficha **Configuración**, en **Administración del tráfico** > **Conmutación de contenido** > **Servidores virtuales**.

> **Importante:**
>
> Al actualizar el entorno de Unified Gateway a la versión 13.0 build 58.x o posterior, el mando DTLS se inhabilita en el servidor virtual de conmutación de contenido configurado antes de la puerta de enlace o el servidor virtual VPN. Habilite manualmente el mando DTLS en el servidor virtual de conmutación de contenido después de la actualización. No habilite el mando DTLS si utiliza el asistente de configuración.

Servidor virtual VPN

El resto de parámetros, perfiles y enlaces de directivas de VPN para la configuración de Unified Gateway se administran en este servidor virtual, incluida la configuración de autenticación principal. Esta entidad se administra en la ficha **Configuración** de **NetScaler Gateway** > **Servidores virtuales**. El nombre del servidor virtual VPN correspondiente incluye el nombre asignado al servidor virtual de Content Switching durante la configuración inicial de Unified Gateway.

> **Nota:**
>
> Los servidores virtuales VPN creados para una implementación de Unified Gateway no son direccionables y tienen asignada la dirección IP 0.0.0.0.

Preguntas frecuentes acerca Gateway unificado

March 27, 2024

¿Qué es Gateway unificado?

Gateway unificado es una nueva función de la versión NetScaler 11.0, que proporciona la capacidad de recibir tráfico en un único servidor virtual (denominado servidor virtual de Gateway unificado) y, a continuación, dirigir internamente ese tráfico, según corresponda, a los servidores virtuales enlazados al servidor virtual de Gateway unificado.

La función de Gateway unificado permite a los usuarios finales acceder a varios servicios mediante una única dirección IP o URL (asociada con el servidor virtual de Gateway unificado). Los administradores pueden liberar direcciones IP y simplificar la configuración de la implementación de NetScaler Gateway.

Cada servidor virtual de Gateway unificado puede front-end un servidor virtual de NetScaler Gateway junto con cero o más servidores virtuales de equilibrio de carga como parte de una formación. Gateway unificado funciona mediante la función de cambio de contenido del dispositivo NetScaler.

Algunos ejemplos de implementaciones de Gateway unificado:

- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway]
- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway, un servidor virtual de equilibrio de carga]
- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway, dos servidores virtuales de equilibrio de carga]

- Servidor virtual de Gateway unificado -> [un servidor virtual de NetScaler Gateway, tres servidores virtuales de equilibrio de carga]

Cada uno de los servidores virtuales de equilibrio de carga puede ser cualquier servidor de equilibrio de carga estándar que aloja un servicio back-end, como Microsoft Exchange o Citrix ShareFile.

¿Por qué utilizar Gateway unificado?

La función Gateway unificado permite a los usuarios finales acceder a varios servicios mediante una única dirección IP o URL (asociada al servidor virtual de Gateway unificado). Para los administradores, la ventaja es que pueden liberar direcciones IP y simplificar la configuración de la implementación de NetScaler Gateway.

¿Puede haber más de un servidor virtual de Gateway unificado?

Sí. Puede haber tantos servidores virtuales de Gateway unificado como necesite.

¿Por qué es necesario cambiar de contenido para Gateway unificado?

La función de conmutación de contenido es necesaria porque el servidor virtual de conmutación de contenido es el que recibe tráfico y lo dirige internamente al servidor virtual apropiado. El servidor virtual de conmutación de contenido es el componente principal de la función de Gateway unificado.

En las versiones anteriores a la 11.0, la conmutación de contenido se puede utilizar para recibir tráfico de varios servidores virtuales. ¿Ese uso también se llama Gateway unificado?

El uso de un servidor virtual de conmutación de contenido para recibir tráfico de varios servidores virtuales se admite en las versiones anteriores a la 11.0. Sin embargo, el cambio de contenido no puede dirigir el tráfico a un servidor virtual de NetScaler Gateway.

Las mejoras de la versión 11.0 permiten que un servidor virtual de conmutación de contenido dirija el tráfico a cualquier servidor virtual, incluido un servidor virtual de NetScaler Gateway.

¿Qué ha cambiado con las directivas de cambio de contenido de Gateway unificado?

1. Se agrega un nuevo parámetro de línea de comandos “-TargetVServer”para la acción de conmutación de contenido. El nuevo parámetro se utiliza para especificar el servidor virtual de NetScaler Gateway de destino. Ejemplo:


```
add cs action ug_CSact_myug -targetvServer ug_VPN_myug
```

En la utilidad de configuración de NetScaler Gateway, la acción de cambio de contenido tiene una nueva opción, Servidor virtual de destino, que puede hacer referencia a un servidor virtual de NetScaler Gateway.

2. Se puede usar una nueva expresión de directiva avanzada, is_vpn_url, para hacer coincidir las solicitudes específicas de autenticación y NetScaler Gateway.

¿Qué funciones de NetScaler Gateway no se admiten actualmente en Gateway unificado?

Todas las funciones son compatibles con Gateway unificado. Sin embargo, se ha notificado un problema menor (ID de problema 544325) con el inicio de sesión nativo a través del complemento VPN. En este caso, el inicio de sesión único (SSO) transparente no funciona.

Con Gateway unificado, ¿cuál es el comportamiento de los análisis de la EPA?

Con Gateway unificado, el análisis de endpoints se desencadena solo para los métodos de acceso de NetScaler Gateway, no para el acceso NetScaler AAA TM. Si un usuario intenta acceder a un servidor virtual de NetScaler AAA TM aunque la autenticación se realiza en el servidor virtual de NetScaler Gateway, el análisis EPA no se desencadena. Sin embargo, si el usuario intenta obtener acceso VPN sin cliente o VPN completa, se desencadena el análisis EPA configurado. En ese caso, se realiza la autenticación o el inicio de sesión único sin interrupciones.

¿Cuáles son los requisitos de licencia de Gateway unificado?

Gateway unificado solo es compatible con las licencias Advanced y Premium. No está disponible solo para NetScaler Gateway ni para las ediciones de licencia estándar.

¿El servidor virtual de NetScaler Gateway utilizado con Gateway unificado necesita una configuración IP/puerto/SSL?

Para un servidor virtual de NetScaler Gateway utilizado con el servidor virtual de Gateway unificado, no se necesita una configuración IP/puerto/SSL en el servidor virtual de NetScaler Gateway. Sin embargo, para la funcionalidad del proxy RDP, puede enlazar el mismo certificado de servidor SSL/TLS al servidor virtual de NetScaler Gateway.

¿Tengo que volver a aprovisionar los certificados SSL/TLS del servidor virtual de NetScaler Gateway para utilizarlos con un servidor virtual de Gateway unificado?

No es necesario volver a aprovisionar los certificados que están vinculados actualmente al servidor virtual de NetScaler Gateway. Puede reutilizar cualquier certificado SSL existente y vincularlo al servidor virtual de Gateway unificado.

¿Cuál es la diferencia entre una única URL y una implementación de varios hosts? ¿Cuál necesito?

La URL única hace referencia a la capacidad del servidor virtual de Gateway unificado para gestionar el tráfico de un nombre de dominio completo (FQDN). Esta restricción existe cuando Gateway unificado utiliza un certificado de servidor SSL/TLS en el que el sujeto del certificado se rellena con el FQDN. Por ejemplo: ug.citrix.com

Si Gateway unificado utiliza un certificado de servidor comodín, puede gestionar el tráfico de varios subdominios. Por ejemplo: *.citrix.com

Otra opción es la configuración SSL/TLS con funcionalidad Indicador de nombre de servidor (SNI) para permitir el enlace de varios certificados de servidor SSL/TLS. Ejemplos: auth.citrix.com, auth.citrix.de, auth.citrix.co.uk, auth.citrix.co.jp

Un host único frente a varios hosts es análogo a la forma en que los sitios web se alojan normalmente en un servidor web (por ejemplo, el servidor HTTP Apache o Microsoft Internet Information Services (IIS)). Si hay un único host, puede utilizar una ruta de acceso del sitio para cambiar el tráfico de la misma manera que utiliza el alias o el "directorio virtual"en Apache. Si hay varios hosts, utiliza un encabezado de host para cambiar el tráfico de forma similar a como usa los hosts virtuales en Apache.

¿Qué mecanismos de autenticación se pueden utilizar con Gateway unificado?

Todos los mecanismos de autenticación existentes compatibles con NetScaler Gateway también son compatibles con Gateway unificado.

Estos incluyen LDAP, RADIUS, SAML, Kerberos, autenticación basada en certificados, etc.

Cualquier mecanismo de autenticación configurado en el servidor virtual de NetScaler Gateway antes de la actualización se utiliza automáticamente cuando el servidor virtual de NetScaler Gateway se coloca detrás del servidor virtual de Gateway unificado. No hay pasos de configuración adicionales que no sean asignar una dirección IP no direccionable (0.0.0.0) al servidor virtual de NetScaler Gateway.

¿Qué es la autenticación"SelfAuth"?

SelfAuth no es un tipo de autenticación por sí solo. SelfAuth describe cómo se crea una URL. Un nuevo parámetro de línea de comandos `ssotype`, está disponible para la configuración de URL de VPN. Ejemplo:

```
> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -
ssotype selfauth
```

SelfAuth es uno de los valores del parámetro `ssotype`. Este tipo de URL se puede utilizar para acceder a recursos que no están en el mismo dominio que el servidor virtual de Gateway unificado. El ajuste se puede ver en la utilidad de configuración al configurar un marcador.

¿Qué es la autenticación"StepUp"?

Cuando se requieren niveles de autenticación adicionales y más seguros para acceder a un recurso NetScaler AAA TM, puede usar la autenticación StepUp. En la línea de comandos, utilice un comando authnProfile para establecer el parámetro AuthenticationLevel. Ejemplo:

```
1 add authentication authnProfile AuthProfile -authnVsName AAATMVserver -
     AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab
     **-**AuthenticationLevel 100
2 <!--NeedCopy-->
```

Este perfil de autenticación está enlazado al servidor virtual de equilibrio de carga.

¿Se admite la autenticación StepUp para los servidores virtuales NetScaler AAA TM?

Sí, es compatible.

¿Qué es `login once/logout once`?

`Login Once`: los usuarios de VPN inician sesión una vez en un servidor virtual de NetScaler AAA TM o NetScaler Gateway. Y a partir de ese momento, los usuarios de VPN tienen acceso sin problemas a todas las aplicaciones empresariales, en la nube y web. No es necesario volver a autenticar al usuario. Sin embargo, la reautenticación se realiza en casos especiales, como NetScaler AAA TM StepUp.

`Logout Once`: Después de crear la primera sesión de NetScaler AAA TM o NetScaler Gateway, se utiliza para crear sesiones posteriores de NetScaler AAA TM o NetScaler Gateway para ese usuario. Si se cierra la sesión de alguna de esas sesiones, el dispositivo NetScaler también cierra la sesión de las demás aplicaciones o sesiones del usuario.

¿Se pueden especificar directivas de autenticación comunes en el nivel de Gateway unificado con el equilibrio de carga de NetScaler AAA TM con enlace autenticado específico del servidor virtual de equilibrio de carga en el nivel del servidor virtual de equilibrio de carga? ¿Cuáles son los pasos de configuración para admitir este caso de uso?

Si necesita especificar directivas de autenticación independientes para el servidor virtual de NetScaler AAA TM detrás de Gateway unificado, debe tener un servidor virtual de autenticación independiente y direccionable de forma independiente (similar a la configuración normal de NetScaler AAA TM). La configuración del host de autenticación del servidor virtual de equilibrio de carga debe apuntar a este servidor virtual de autenticación.

¿Cómo se configura Gateway unificado para que los servidores virtuales NetScaler AAA TM vinculados tengan sus propias directivas de autenticación?

En este caso, el servidor de equilibrio de carga debe tener la opción FQDN de autenticación establecida para que apunte al servidor virtual de NetScaler AAA TM. El servidor virtual de NetScaler AAA TM debe tener una dirección IP independiente y ser accesible desde NetScaler y los clientes.

¿Se necesita un servidor virtual de autenticación NetScaler AAA TM para autenticar a los usuarios que llegan a través de un servidor virtual de Gateway unificado?

No. El servidor virtual de NetScaler Gateway autentica incluso a los usuarios de NetScaler AAA TM.

¿Dónde se especifican las directivas de autenticación de NetScaler Gateway, en el servidor virtual de Gateway unificado o en el servidor virtual de NetScaler Gateway?

Las directivas de autenticación deben vincularse al servidor virtual de NetScaler Gateway.

¿Cómo habilita la autenticación en los servidores virtuales NetScaler AAA TM detrás de un servidor virtual de conmutación de contenido de Gateway unificado?

Habilite la autenticación en NetScaler AAA TM y apunte el host de autenticación al FQDN de conmutación de contenido de Gateway unificado.

¿Cómo agrego servidores virtuales de TM para el cambio de contenido (URL única o multihost)?

No hay diferencia entre agregar los servidores virtuales NetScaler AAA TM para una única URL y agregarla para varios hosts. En cualquier caso, el servidor virtual se agrega como destino en una acción de cambio de contenido. La diferencia entre una URL única y un host múltiple se implementa mediante reglas de directiva de conmutación de contenido.

¿Qué sucede con las directivas de autenticación vinculadas a un servidor virtual de equilibrio de carga NetScaler AAA TM si ese servidor virtual se mueve detrás de un servidor virtual de Gateway unificado?

Las directivas de autenticación están vinculadas al servidor virtual de autenticación y el servidor virtual de autenticación está enlazado al servidor virtual de equilibrio de carga. Para el servidor virtual de Gateway unificado, Citrix recomienda tener el servidor virtual de NetScaler Gateway como punto de autenticación único, lo que niega la necesidad de realizar la autenticación en un servidor virtual de autenticación (o incluso la necesidad de un servidor virtual de autenticación específico). Apuntar el host de autenticación al FQDN del servidor virtual de Gateway unificado garantiza que el servidor virtual de NetScaler Gateway realice la autenticación. Si apunta el host de autenticación al cambio de contenido de Gateway unificado y sigue teniendo un servidor virtual de autenticación vinculado, se ignoran las directivas de autenticación vinculadas al servidor virtual de autenticación. Sin embargo, si apunta un host de autenticación a un servidor virtual de autenticación direccionable independiente, surten efecto las directivas de autenticación vinculadas.

¿Cómo se configuran las directivas de sesión para las sesiones de NetScaler AAA TM?

Si, en Gateway unificado, no se especifica ningún servidor virtual de autenticación para el servidor virtual de NetScaler AAA TM, las sesiones de NetScaler AAA TM heredan las directivas de sesión de NetScaler Gateway. Si se especifica el servidor virtual de autenticación, se aplican las directivas de sesión de NetScaler AAA TM enlazadas a ese servidor virtual.

¿Cuáles son los cambios en el portal de NetScaler Gateway en NetScaler 11.0?

En las versiones de NetScaler anteriores a la 11.0, se puede configurar una única personalización del portal a nivel global. Todos los servidores virtuales de puerta de enlace de un dispositivo NetScaler determinado utilizan la personalización del portal global.

En NetScaler 11.0, con la función de temas del portal, puede configurar varios temas del portal. Los temas se pueden enlazar de forma global o a servidores virtuales específicos.

¿NetScaler 11.0 admite la personalización del portal de NetScaler Gateway?

Con la utilidad de configuración, puede utilizar la nueva función de temas del portal para personalizar y crear los temas del portal por completo. Puede subir diferentes imágenes, establecer esquemas de color, cambiar etiquetas de texto, etc.

Las páginas del portal que se pueden personalizar son:

- Página de inicio
- Página Análisis de endpoint
- Página Error de Análisis de Endpoint
- Página Post Endpoint Analysis
- Página Conexión VPN
- Página de inicio del portal

Con esta versión, puede personalizar los servidores virtuales de NetScaler Gateway con diseños de portal únicos.

¿Los temas del portal se admiten en implementaciones de clústeres o de alta disponibilidad de NetScaler?

Sí. Los temas del portal se admiten en implementaciones de clústeres y alta disponibilidad de NetScaler.

¿Se migran mis personalizaciones como parte del proceso de actualización de NetScaler 11.0?

No. Las personalizaciones existentes en la página del portal de NetScaler Gateway que se invocan mediante la modificación del archivo rc.conf/rc.netscaler o mediante la funcionalidad de temas personalizados en 10.1/10.5 no se migrarán automáticamente al actualizar a NetScaler 11.0.

¿Hay que seguir algún paso previo a la actualización para estar preparado para los temas del portal en NetScaler 11.0?

Todas las personalizaciones existentes deben eliminarse de los archivos rc.conf o rc.netscaler.

La otra opción es que si se utilizan temas personalizados, se les debe asignar el ajuste Predeterminado:

1. Vaya a **Configuración > NetScaler Gateway > Configuración global**
2. Haga clic en **Cambiar configuración global**.

3. Haga clic en **Experiencia del cliente** y seleccione **Predeterminado** en la lista **Tema de interfaz** de usuario.

Tengo personalizaciones almacenadas en la instancia de NetScaler, invocadas por rc.conf o rc.netscaler. ¿Cómo paso a los temas del portal?

El artículo CTX126206 de Citrix Knowledge Center detalla esta configuración para las versiones 9.3 y 10.0 de NetScaler hasta 10.0 build 73.5001.e. Desde NetScaler 10.0, compilación 10.0 73.5002.e (incluidas 10.1 y 10.5), el parámetro UITHEME CUSTOM ha estado disponible para ayudar a los clientes a conservar sus personalizaciones durante los reinicios. Si las personalizaciones se almacenan en el disco duro de NetScaler y quiere seguir usando estas personalizaciones, respalde los archivos GUI de la versión 11.0 e insértelos en el archivo de tema personalizado existente. Si desea pasar a los temas del portal, primero debe desactivar el parámetro UITHEME en la configuración global o en el perfil de sesión, en Experiencia de **cliente**. O bien puede configurarlo como DEFAULT o GREENBUBBLE. A continuación, podrá empezar a crear y enlazar un tema de portal.

¿Cómo puedo exportar mis personalizaciones actuales y guardarlas antes de actualizar a NetScaler 11.0? ¿Puedo mover los archivos exportados a otro dispositivo NetScaler?

Los archivos personalizados que se han cargado en la carpeta **ns_gui_custom** están en el disco y persisten durante las actualizaciones. Sin embargo, es posible que estos archivos no sean totalmente compatibles con el nuevo kernel de NetScaler 11.0 y otros archivos GUI que forman parte del núcleo. Por lo tanto, Citrix recomienda hacer una copia de seguridad de los archivos GUI de la versión 11.0 y personalizar las copias de seguridad.

Además, no hay ninguna utilidad en la utilidad de configuración para exportar la carpeta **ns_custom_gui** a otro dispositivo NetScaler. Utilice SSH o una utilidad de transferencia de archivos como WinSCP para quitar los archivos de la instancia de NetScaler.

¿Los temas del portal son compatibles con los servidores virtuales NetScaler AAA TM?

Sí. Los temas del portal son compatibles con los servidores virtuales NetScaler AAA TM.

¿Qué ha cambiado en la función Proxy RDP de NetScaler Gateway 11.0?

Se han realizado muchas mejoras en RDP Proxy desde la versión de mejora de NetScaler 10.5.e. En NetScaler 11.0, esta función está disponible desde la primera compilación publicada.

Cambios en las licencias

La función RDP Proxy de NetScaler 11.0 solo se puede utilizar con las ediciones Premium y Advanced. Se deben obtener licencias de usuario simultáneo (CCU) de Citrix para cada usuario.

Habilitar comando

En NetScaler 10.5.e no había ningún comando para habilitar el proxy RDP. En NetScaler 11.0, se ha agregado el comando enable:

```
enable feature rdpproxy
<!--NeedCopy-->
```

La función debe tener licencia para ejecutar este comando.

Otros cambios en el proxy RDP

Se ha convertido en obligatorio un atributo de clave previamente compartida (PSK) en el perfil del servidor.

Para migrar las configuraciones existentes de NetScaler 10.5.e para el proxy RDP a NetScaler 11.0, se deben comprender y abordar los siguientes detalles.

Si un administrador quiere agregar una configuración de proxy RDP existente a una implementación de Gateway unificado elegida:

- La dirección IP del servidor virtual de NetScaler Gateway debe modificarse y establecerse en una dirección IP no direccionable (0.0.0.0).
- Los certificados de servidor SSL/TLS y las directivas de autenticación deben estar vinculados al servidor virtual de NetScaler Gateway que forma parte de la formación de Gateway unificado elegida.

¿Cómo se migra una configuración de proxy del Protocolo de escritorio remoto (RDP) basada en NetScaler 10.5.e a NetScaler 11.0?

Opción 1: Mantenga el servidor virtual de NetScaler Gateway existente con la configuración de proxy RDP tal cual, con una licencia Premium o Advanced.

Opción 2: Mueva el servidor virtual de NetScaler Gateway existente con la configuración de proxy RDP y colóquelo detrás de un servidor virtual de Gateway unificado.

Opción 3: Agregar un servidor virtual de NetScaler Gateway independiente con configuración de proxy RDP a un dispositivo Standard Edition existente.

¿Cómo se configura la configuración del proxy de NetScaler Gateway para RDP mediante la versión NetScaler 11.0?

Existen dos opciones para implementar el proxy RDP mediante la versión NS 11.0:

1. Uso de un servidor virtual de NetScaler Gateway externo. Esto requiere una dirección IP/FQDN visible externamente para el servidor virtual de NetScaler Gateway. Esta opción es la que está disponible en NetScaler 10.5.e.
2. Utilizar un servidor virtual de Gateway unificado para front-end del servidor virtual de NetScaler Gateway.

Con la opción 2, el servidor virtual de NetScaler Gateway no necesita su propia dirección IP/FQDN, porque utiliza una dirección IP no direccionable (0.0.0.0).

¿HDX Insight es compatible con Gateway unificado?

Cuando NetScaler Gateway se implementa con Gateway unificado, se deben cumplir las siguientes condiciones:

- El servidor virtual de NetScaler Gateway debe tener un certificado SSL válido vinculado a él.
- El servidor virtual de NetScaler Gateway debe estar activo para generar registros de AppFlow en NetScaler ADM y generar informes de HDX Insight.

¿Cómo migro mi configuración HDX Insight existente?

No es necesaria ninguna migración. Las directivas de AppFlow vinculadas a un servidor virtual de NetScaler Gateway se trasladan si ese servidor virtual de NetScaler Gateway se coloca detrás de un servidor virtual de Gateway unificado.

Para los datos existentes en NetScaler ADM para el servidor virtual de NetScaler Gateway, hay dos posibilidades:

- Si la dirección IP del servidor virtual de NetScaler Gateway se asigna a un servidor virtual de Gateway unificado como parte de la migración a Gateway unificado, los datos permanecen vinculados al servidor virtual de NetScaler Gateway.
- Si al servidor virtual de Gateway unificado se le asigna una dirección IP independiente, los datos de AppFlow del servidor virtual de NetScaler Gateway se vinculan a esa nueva dirección IP. Por lo tanto, los datos existentes no forman parte de los datos nuevos.

Configuración de VPN en un dispositivo NetScaler Gateway

March 27, 2024

> **Importante:**
>
> Las capturas de pantalla de esta sección se mantienen en escala de grises por los siguientes motivos:
>
> - Ayude a los lectores con discapacidad visual, especialmente a aquellos con daltonismo o deficiencia de color.
> - El uso de una imagen en escala de grises representa la imagen de forma genérica que no muestra ningún impacto en la personalización del código de colores que podría haberse realizado en el explorador del usuario o en el sistema operativo.

Los usuarios pueden utilizar los siguientes métodos para conectarse a los recursos de red de su organización a través de NetScaler Gateway:

- Aplicación Citrix Workspace que contiene todos los complementos de Citrix instalados en el dispositivo del usuario.
- Aplicación Citrix Workspace para web que permite conexiones de usuario a aplicaciones, escritorios y ShareFile mediante un explorador web.
- Secure Hub para permitir a los usuarios acceder a Secure Mail, WorxWeb y aplicaciones móviles desde sus dispositivos iOS y Android.
- Cliente Citrix Secure Access para Windows, macOS X o Linux.
- Aplicación NetScaler Gateway para iOS y Android.
- Acceso sin cliente que proporciona a los usuarios el acceso que necesitan sin instalar software de usuario.
- Interoperabilidad con el complemento Citrix SD-WAN.

Si los usuarios instalan el cliente Citrix Secure Access y, a continuación, instalan la aplicación Citrix Workspace desde Citrix Virtual Apps 6.5 para Windows Server 2008 (incluidos el Feature Pack y el Feature Pack 2), Citrix Virtual Desktops 7.0 o versiones posteriores, la aplicación Citrix Workspace agrega automáticamente el cliente Citrix Secure Access. Los usuarios pueden conectarse con el cliente Citrix Secure Access desde un navegador web o desde la aplicación Citrix Workspace.

SmartAccess determina automáticamente los métodos de acceso permitidos para un dispositivo de usuario en función de los resultados de un análisis de puntos finales. Para obtener más información sobre SmartAccess, consulte Configuración de SmartAccess.

NetScaler Gateway admite las aplicaciones móviles de productividad de Citrix Endpoint Management para dispositivos móviles iOS y Android. NetScaler Gateway contiene Secure Browse que permite las conexiones a NetScaler Gateway desde dispositivos móviles iOS que establecen el túnel micro VPN.

Los dispositivos Android que se conectan con Secure Hub también establecen automáticamente un túnel micro VPN que proporciona acceso seguro a nivel de aplicaciones web y móviles a los recursos de su red interna. Si los usuarios se conectan desde un dispositivo Android con aplicaciones móviles de productividad, debe configurar la configuración de DNS en NetScaler Gateway. Para obtener más información, consulte Compatibilidad con consultas DNS mediante sufijos DNS para dispositivos Android.

Cómo se conectan los usuarios con el cliente Citrix Secure Access

March 27, 2024

NetScaler Gateway funciona de la siguiente manera:

- Cuando los usuarios intentan acceder a los recursos de la red a través del túnel VPN, el cliente Citrix Secure Access cifra todo el tráfico de red destinado a la red interna de la organización y reenvía los paquetes a NetScaler Gateway.
- NetScaler Gateway finaliza el túnel SSL, acepta cualquier tráfico entrante destinado a la red privada y reenvía el tráfico a la red privada. NetScaler Gateway devuelve el tráfico al equipo remoto a través de un túnel seguro.

Cuando los usuarios escriben la dirección web, reciben una página de inicio de sesión en la que introducen sus credenciales e inician sesión. Si las credenciales son correctas, NetScaler Gateway finaliza el enlace con el dispositivo del usuario.

Si el usuario se conecta a través de un servidor proxy, puede especificar tanto el servidor proxy como las credenciales de autenticación. Para obtener más información, consulte Habilitación de la compatibilidad con proxy para conexiones de usuario.

El cliente Citrix Secure Access está instalado en el dispositivo del usuario. Tras la primera conexión, si los usuarios inician sesión con un equipo basado en Windows, pueden usar el icono del área de notificación para establecer la conexión.

Establezca el túnel seguro

Cuando los usuarios se conectan con el cliente Citrix Secure Access, Secure Hub o la aplicación Citrix Workspace, el software del cliente establece un túnel seguro a través del puerto 443 (o cualquier puerto configurado de NetScaler Gateway) y envía la información de autenticación. Cuando se establece el túnel, NetScaler Gateway envía información de configuración al cliente Citrix Secure Access, Secure Hub o la aplicación Citrix Workspace en la que se describen las redes que se van a proteger y contiene una dirección IP si se habilitan los grupos de direcciones.

Túnel del tráfico de red privada a través de conexiones seguras

Cuando se inicia el cliente Citrix Secure Access y se autentica al usuario, todo el tráfico de red destinado a redes privadas especificadas se captura y se redirige a través del túnel seguro a NetScaler Gateway. La aplicación Citrix Workspace debe admitir que el cliente Citrix Secure Access establezca la conexión a través del túnel seguro cuando los usuarios inicien sesión.

Secure Hub, Secure Mail y WorxWeb utilizan Micro VPN para establecer el túnel seguro para dispositivos móviles iOS y Android.

NetScaler Gateway intercepta todas las conexiones de red que realiza el dispositivo del usuario y las multiplexa a través de Secure Sockets Layer (SSL) a NetScaler Gateway, donde el tráfico se demultiplexa y las conexiones se reenvían a la combinación correcta de host y puerto.

Las conexiones están sujetas a directivas de seguridad administrativas que se aplican a una única aplicación, a un subconjunto de aplicaciones o a toda una intranet. Especifica los recursos (intervalos de pares de direcciones IP/subred) a los que los usuarios remotos pueden acceder a través de la conexión VPN.

El cliente Citrix Secure Access intercepta y canaliza los siguientes protocolos para las aplicaciones de intranet definidas:

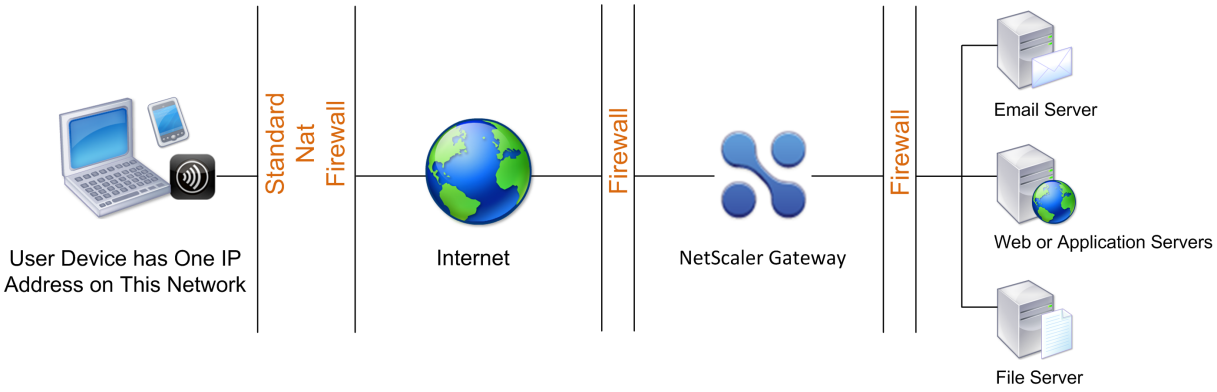
- TCP (todos los puertos)
- UDP (todos los puertos)
- ICMP (tipos 8 y 0 - solicitud/respuesta de eco)

Las conexiones de las aplicaciones locales del dispositivo del usuario se tunelizan de forma segura a NetScaler Gateway, que restablece las conexiones con el servidor de destino. Los servidores de destino consideran que las conexiones se originan en el NetScaler Gateway local de la red privada, ocultando así el dispositivo del usuario. Esto también se denomina traducción inversa de direcciones de red (NAT). Ocultar direcciones IP agrega seguridad a las ubicaciones de origen.

A nivel local, en el dispositivo del usuario, el cliente Citrix Secure Access recrea todo el tráfico relacionado con la conexión, como los paquetes SYN-ACK, PUSH, ACK y FIN, para que aparezca en el servidor privado.

Conéctese a través de firewalls y proxies

Los usuarios del cliente Citrix Secure Access a veces se encuentran dentro del firewall de otra organización, como se muestra en la siguiente figura:



Los firewalls NAT mantienen una tabla que les permite redirigir paquetes seguros desde NetScaler Gateway de vuelta al dispositivo del usuario. Para las conexiones orientadas a circuitos, NetScaler Gateway mantiene una tabla de traducción NAT inversa asignada a puertos. La tabla de traducción NAT inversa permite a NetScaler Gateway hacer coincidir las conexiones y enviar paquetes de vuelta por el túnel al dispositivo de usuario con los números de puerto correctos para que los paquetes regresen a la aplicación correcta.

Controle la actualización de los clientes de Citrix Secure Access

Los administradores del sistema controlan el rendimiento del plug-in de NetScaler cuando su versión no coincide con la revisión de NetScaler Gateway. Las nuevas opciones controlan el comportamiento de actualización de plug-ins para Mac y Windows o sistemas operativos.

En el caso de los plug-ins VPN, la opción de actualización se puede establecer en dos lugares de la interfaz de usuario del dispositivo NetScaler:

- En la configuración global
- En el nivel de perfil de sesión

Requisitos

- La versión del complemento VPN y EPA de Windows debe ser superior a 11.0.0.0
- La versión del complemento EPA para Mac debe ser superior a 3.0.0.31
- La versión del complemento VPN para Mac debe ser superior a la 3.1.4 (357)

> **Nota:**
>
> Si el dispositivo NetScaler se actualiza a la versión 11.0, todos los plug-ins VPN (y EPA) anteriores se actualizan a la última versión, independientemente de la configuración del control de

> actualizaciones. Para las actualizaciones posteriores, respetan la configuración de control de actualización anterior.

Comportamientos de plug-ins

Para cada tipo de cliente, NetScaler Gateway permite las tres opciones siguientes para controlar el comportamiento de actualización de plug-ins:

- **Siempre**

El complemento siempre se actualiza cuando la versión del complemento del usuario final no coincide con el complemento suministrado con el dispositivo NetScaler. Este es el comportamiento predeterminado. Elija esta opción si no quiere que se ejecuten varias versiones de plug-ins en su empresa.

- **Esencial** (y seguridad)

El plug-in solo se actualiza cuando se considera necesario. Los ascensos de clase se consideran necesarios en las dos circunstancias siguientes:

- El complemento instalado no es compatible con la versión actual del dispositivo NetScaler.
- El complemento instalado debe actualizarse para obtener la solución de seguridad necesaria.

Elija esta opción si quiere minimizar el número de actualizaciones de plug-ins, pero no quiere perderse ninguna actualización de seguridad de plug-ins

- **Nunca**

El plug-in no se actualiza.

Parámetros CLI para controlar la actualización de plug-ins VPN

NetScaler Gateway admite dos tipos de complementos (EPA y VPN) para sistemas operativos Windows y Mac. Para admitir el control de actualización de plug-ins VPN a nivel de sesión, NetScaler Gateway admite dos parámetros de perfil de sesión denominados WindowsInPluginUpgrade y MacPluginUpgrade.

Estos parámetros están disponibles a nivel global, servidor virtual, grupo y usuario. Cada parámetro puede tener el valor Always, Essential o Never. Para obtener una descripción de estos parámetros, consulte Comportamientos de plug-ins.

Parámetros CLI para controlar la actualización de plug-ins de EPA

NetScaler Gateway admite complementos EPA para sistemas operativos Windows y Mac. Para admitir el control de actualización de plug-ins de EPA a nivel de servidor virtual, NetScaler Gateway admite dos parámetros de servidor virtual denominados windowsEPAPluginUpgrade y macEPAPluginUpgrade.

Los parámetros están disponibles en el nivel del servidor virtual. Cada parámetro puede tener el valor Always, Essential o Never. Para obtener una descripción de estos parámetros, consulte Comportamientos de plug-in

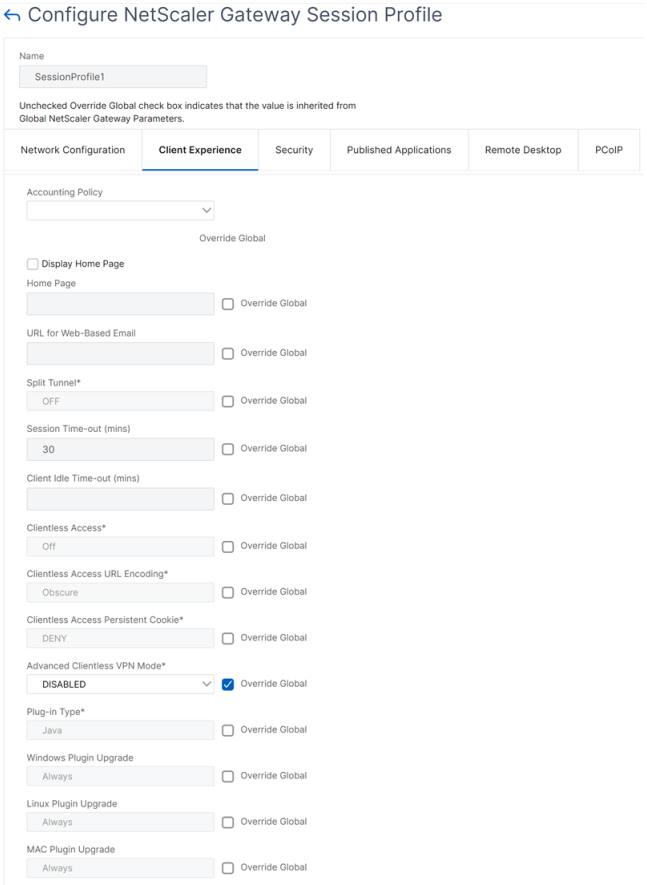
Configuración VPN

Siga estos pasos para **configurar la VPN de los complementos de** Windows, Linux y Mac.

1. Vaya a **NetScaler > Directivas > Sesión.**
2. Seleccione la directiva de sesión deseada y, a continuación, haga clic en **Modificar**.
3. Seleccione la ficha **Experiencia del cliente**.
4. Estas opciones de cuadros de diálogo afectan al comportamiento de actualización.

   - Siempre
   - Esencial
   - Nunca

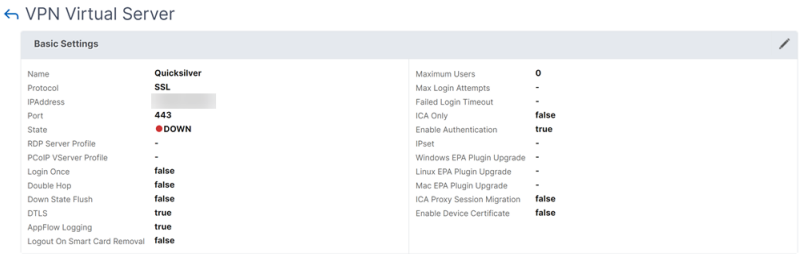
   El valor predeterminado es Siempre.
5. Seleccione la casilla de verificación situada a la derecha de cada opción. Seleccione la frecuencia para aplicar el comportamiento de actualización.



Configuración de la EPA

Siga estos pasos para la configuración de la EPA de los complementos de Windows, Linux y Apple.

1. Vaya a **NetScaler Gateway > Servidores virtuales**.
2. Seleccione un servidor y haga clic en el botón **Modificar**.
3. Haga clic en el icono del **lápiz**.



4. Haga clic en **Más**
5. Los cuadros de diálogo que aparecen afectan al comportamiento de la actualización. Las opciones disponibles son:

- Siempre
- Esencial
- Nunca

Configuración de VPN completa en NetScaler Gateway

March 27, 2024

En esta sección se describe cómo configurar la configuración completa de VPN en un dispositivo NetScaler Gateway. Contiene consideraciones sobre redes y el enfoque ideal para resolver problemas desde la perspectiva de la red.

Requisitos previos

- Instale un certificado SSL y vincúlelo al servidor virtual VPN.
  - CTX109260: Cómo generar e instalar un certificado SSL público en un dispositivo NetScaler
  - CTX122521: Cómo reemplazar el certificado predeterminado de un dispositivo NetScaler por un certificado de CA de confianza que coincida con el nombre de host del dispositivo
  - Documentación de NetScaler: enlace del par de claves de certificado alservidor virtual basado en SSL
- Cree un perfil de autenticación para NetScaler Gateway.
  - Para obtener información adicional, consulte la documentación de NetScaler: Configuración de la autenticación de usuario externo
  - Para obtener información adicional, consulte Lista de comprobación: Uso de AD FS para implementar y administrar el inicio de sesión único
- Descarga VPN Client.
- Cree una directiva de sesión que permita conexiones VPN completas.

Cuando los usuarios se conectan con el cliente Citrix Secure Access, Secure Hub o la aplicación Citrix Workspace, el software del cliente establece un túnel seguro a través del puerto 443 (o cualquier puerto configurado de NetScaler Gateway) y envía la información de autenticación. Una vez establecido el túnel, NetScaler Gateway envía la información de configuración al cliente Citrix Secure Access, Citrix Secure Hub o la aplicación Citrix Workspace con la descripción de las redes que se van a proteger. Esta información también contiene una dirección IP si habilita las IP de la intranet.

Las conexiones de dispositivos de usuario se configuran definiendo los recursos a los que los usuarios pueden acceder en la red interna. La configuración de conexiones de dispositivos de usuario incluye lo siguiente:

- Túneles divididos
- Direcciones IP de usuarios, incluidos grupos de direcciones (IP de intranet)
- Conexiones a través de un servidor proxy
- Definición de los dominios a los que se permite el acceso de los usuarios
- Configuración de tiempo de espera
- Single Sign-On
- Software de usuario que se conecta a través de NetScaler Gateway
- Acceso para dispositivos móviles

La mayoría de las conexiones de dispositivos de usuario se configuran mediante un perfil que forma parte de una directiva de sesión. También puede definir la configuración de conexión del dispositivo de usuario mediante directivas de autenticación, tráfico y autorización. También se pueden configurar mediante aplicaciones de intranet.

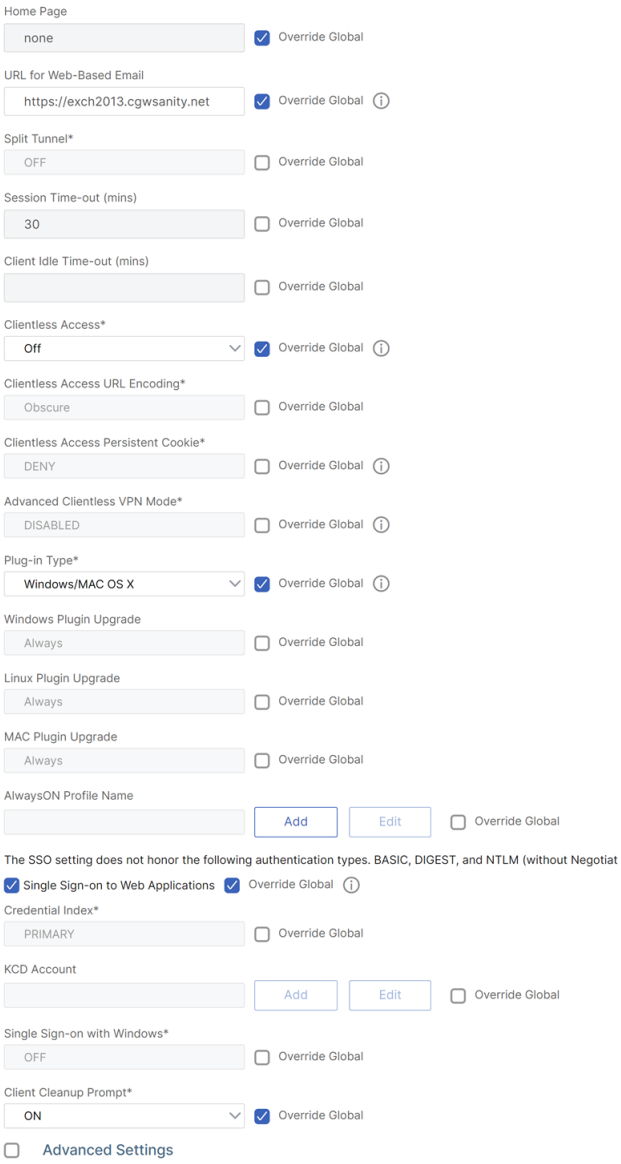
Configurar una configuración VPN completa en un dispositivo NetScaler Gateway

Para configurar una configuración de VPN en el dispositivo NetScaler Gateway, realice el siguiente procedimiento:

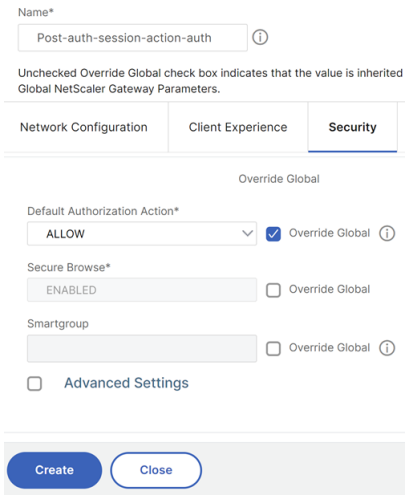
1. Vaya a **Administración del tráfico > DNS**.
2. Seleccione el nodo Servidores de nombres, como se muestra en la siguiente captura de pantalla. Asegúrese de que el servidor de nombres DNS aparece en la lista. Si no está disponible, agregue un servidor de nombres DNS.

3. Expanda **NetScaler Gateway > Directivas**.
4. Seleccione el nodo **Sesión**.
5. En la página Perfiles y directivas de sesión de NetScaler Gateway, haga clic en la ficha **Perfiles** y haga clic en **Agregar**.
   Para cada componente que configure en el cuadro de diálogo Configurar perfil de sesión de NetScaler Gateway, asegúrese de seleccionar la opción **Supedición global** para el componente correspondiente.
6. Haga clic en la ficha **Experiencia del cliente**.

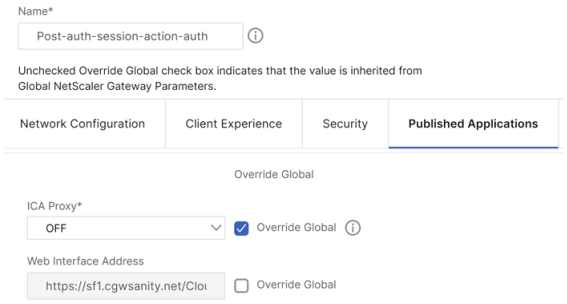
7. Escriba la URL del portal de la intranet en el campo Página de inicio si quiere presentar cualquier URL cuando el usuario inicie sesión en la VPN. Si el parámetro de página de inicio se establece en "nohomepage.html", la página principal no se muestra. Cuando se inicia el plug-in, se inicia una instancia del explorador y se mata automáticamente.
8. Asegúrese de seleccionar la configuración deseada de la lista Túnel dividido.
9. Selecciona **DESACTIVADO** en la lista **Acceso sin cliente** si quieres FullVPN.
10. Asegúrese de que **Windows/Mac OS X** esté seleccionado en la lista **Tipo de plug-in**.
11. Seleccione la opción **Single Sign-On en aplicaciones web** si lo quiere.
12. Asegúrese de que la opción **Mensaje de limpieza del cliente** esté seleccionada si es necesario, como se muestra en la siguiente captura de pantalla:



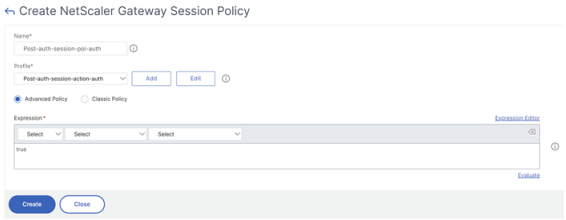
13. Haga clic en la ficha **Seguridad**.
14. Asegúrese de que la opción **PERMITIR** esté seleccionada en la lista de **acciones de autorización predeterminadas** .



15. Haga clic en la ficha **Published Applications**.
16. Asegúrese de que está seleccionado **DESACTIVADO** en la lista **Proxy ICA** de la opción **Aplicaciones publicadas**.



17. Haga clic en **Crear**.
18. Haga clic en **Cerrar**.
19. Haga clic en la ficha **Directivas** de la página Perfiles y directivas de sesión de NetScaler Gateway del servidor virtual o active las Directivas de sesión a nivel de GRUPO/USUARIO según sea necesario.
20. Cree una directiva de sesión con una expresión requerida o true, como se muestra en la siguiente captura de pantalla:

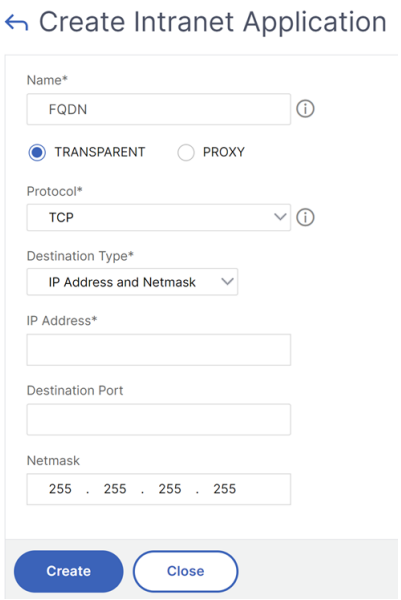


21. Enlazar la directiva de sesión al servidor virtual VPN. Para obtener más información, consulte Vincular directivas de sesión.

    Si el Túnel dividido se activó, debe configurar las aplicaciones de intranet a las que quiere que accedan los usuarios cuando estén conectados a la VPN. Para obtener más información sobre las aplicaciones de intranet, consulte Configurar aplicaciones de intranet para el cliente Citrix Secure Access.

    a) Vaya a **NetScaler Gateway > Recursos > Aplicaciones de intranet**.

    b) Cree una aplicación de intranet. Seleccione Transparente para FullVPN con cliente Windows. Seleccione el protocolo que quiere permitir (TCP, UDP o ANY), el tipo de destino (dirección IP y máscara, intervalo de direcciones IP o nombre de host).



    c) Si es necesario, defina una nueva directiva para VPN en iOS y Android con la siguiente expresión:
    `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")`

    d) Enlazar las aplicaciones de intranet creadas a nivel USER/GRUPO/VSERVER según sea necesario.

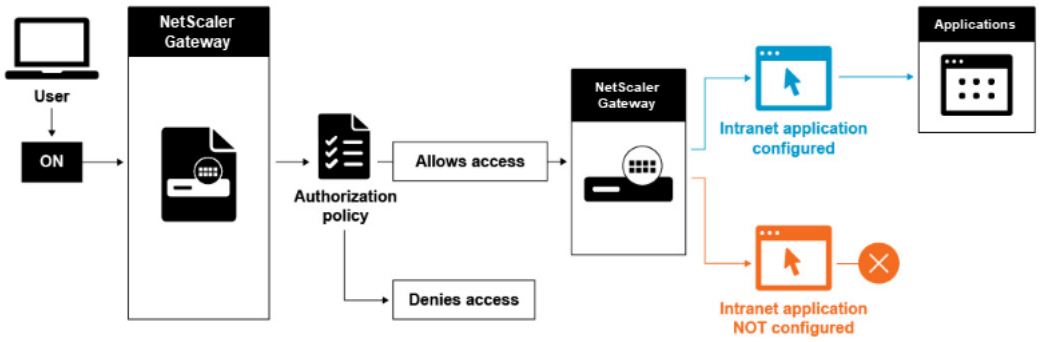
Configurar túnel dividido

1. Vaya a **Configuración** > **NetScaler Gateway > Políticas > Sesión** .
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en **Modificar**.
3. En la ficha **Experiencia del cliente**, junto a **Túnel dividido**, seleccione **Anulación global**, seleccione una opción y, a continuación, haga clic en **Aceptar**.

   Configurar la autorización y la tunelización dividida

   Al planificar la implementación de NetScaler Gateway, es importante tener en cuenta la tunelización dividida y la acción de autorización y las directivas de autorización predeterminadas.

   Por ejemplo, tiene una directiva de autorización que permite el acceso a un recurso de red. La tunelización dividida está activada y no configura las aplicaciones de intranet para enviar tráfico de red a través de NetScaler Gateway. Cuando NetScaler Gateway tiene este tipo de configuración, se permite el acceso al recurso, pero los usuarios no pueden acceder al recurso.



Si la directiva de autorización niega el acceso a un recurso de red, el cliente Citrix Secure Access envía tráfico a NetScaler Gateway, pero se deniega el acceso al recurso en las siguientes condiciones.

- Tiene el túnel dividido configurado en ON.
- Las aplicaciones de intranet están configuradas para dirigir el tráfico de red a través de NetScaler Gateway

Para obtener más información sobre las directivas de autorización, revise lo siguiente:

- Configuración de autorización
- Configuración de directivas de autorización
- Configuración de la autorización global predeterminada

Para configurar el acceso de red a los recursos internos de la red

1. Vaya a **Configuración** > **NetScaler Gateway > Recursos > Aplicaciones de intranet**.

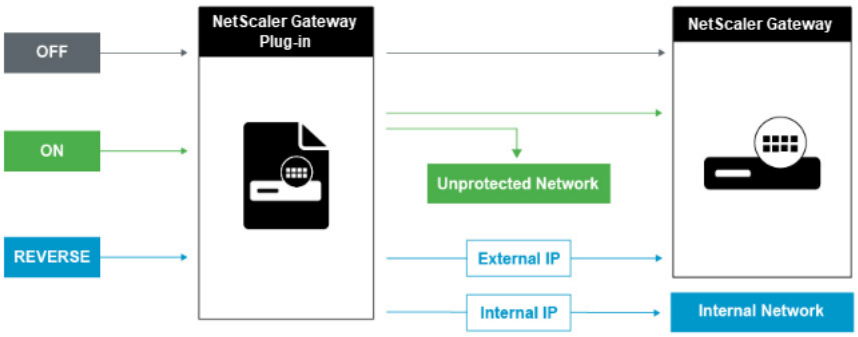
2. En el panel de detalles, haga clic en **Agregar**.
3. Complete los parámetros para permitir el acceso a la red, haga clic en **Crear** y, a continuación, en **Cerrar**.

Cuando no configuramos las IP de la intranet para los usuarios de VPN, el usuario envía el tráfico al VIP de NetScaler Gateway y, a partir de ahí, el dispositivo NetScaler crea un nuevo paquete en el recurso de aplicación de intranet de la LAN interna. Este nuevo paquete se va a obtener desde el SNIP hacia la aplicación de intranet. Desde aquí, la aplicación de intranet obtiene el paquete, lo procesa y, a continuación, intenta responder al origen de ese paquete (el SNIP en este caso). El SNIP recibe el paquete y envía la respuesta al cliente que realizó la solicitud.

Cuando se utiliza una dirección IP de intranet, el usuario envía el tráfico al VIP de NetScaler Gateway y, desde allí, el dispositivo NetScaler asignará la IP del cliente a una de las IP de INTRANET configuradas desde el grupo. Tenga en cuenta que el dispositivo NetScaler va a ser propietario del grupo de IP de la intranet y, por este motivo, estos rangos no deben utilizarse en la red interna. El dispositivo NetScaler asigna una IP de intranet para las conexiones VPN entrantes como lo haría un servidor DHCP. El dispositivo NetScaler crea otro paquete para la aplicación de intranet en la LAN al que accedería el usuario. Este nuevo paquete se va a obtener de una de las IP de la intranet hacia la aplicación de intranet. Desde aquí, las aplicaciones de intranet obtienen el paquete, lo procesan y luego intentan responder al origen de ese paquete (la IP INTRANET). En este caso, el paquete de respuesta debe redirigirse al dispositivo NetScaler, donde se encuentran las IP de INTRANET (recuerde que el dispositivo NetScaler posee las subredes IP de intranet). Para llevar a cabo esta tarea, el administrador de red debe tener una ruta hacia la IP de INTRANET que apunte a uno de los SNIP. Se recomienda redirigir el tráfico hacia el SNIP que contiene la ruta desde la que sale el paquete del dispositivo NetScaler por primera vez para evitar cualquier tráfico asimétrico.

Opciones de tunelización dividida

Estas son las distintas opciones de tunelización dividida.



Túnel dividido APAGADO

Cuando el túnel dividido está desactivado, el cliente Citrix Secure Access captura todo el tráfico de red que se origina en un dispositivo de usuario y lo envía a través del túnel VPN a NetScaler Gateway. En otras palabras, el cliente VPN establece una ruta predeterminada desde el PC cliente que apunta al VIP de NetScaler Gateway, lo que significa que todo el tráfico debe enviarse a través del túnel para llegar al destino. Dado que todo el tráfico se va a enviar a través del túnel, las directivas de autorización deben determinar si se permite el paso del tráfico a los recursos internos de la red o si se deniega.

Si bien está configurado en "desactivado", todo el tráfico pasa por el túnel, incluido el tráfico web estándar a los sitios web. Si el objetivo es supervisar y controlar este tráfico web, debe reenviar estas solicitudes a un proxy externo mediante el dispositivo NetScaler. Los dispositivos de usuario también se pueden conectar a través de un servidor proxy para acceder a redes internas.
NetScaler Gateway admite los protocolos HTTP, SSL, FTP y SOCKS. Para habilitar la compatibilidad con proxy para las conexiones de usuario, debe especificar esta configuración en NetScaler Gateway. Puede especificar la dirección IP y el puerto que utiliza el servidor proxy de NetScaler Gateway. El servidor proxy se utiliza como proxy de reenvío para todas las demás conexiones a la red interna.

Para obtener más información, consulte los siguientes enlaces:

- Habilitación del soporte proxy para conexiones de usuario

Túnel dividido ENCENDIDO

Puede habilitar la tunelización dividida para evitar que el cliente Citrix Secure Access envíe tráfico de red innecesario a NetScaler Gateway. Si el túnel dividido está habilitado, el cliente Citrix Secure Access envía solo el tráfico destinado a las redes protegidas (aplicaciones de intranet) por NetScaler Gateway a través del túnel VPN. El cliente Citrix Secure Access no envía el tráfico de red destinado a redes desprotegidas a NetScaler Gateway. Cuando se inicia el cliente Citrix Secure Access, obtiene la lista de aplicaciones de intranet de NetScaler Gateway y establece una ruta para cada subred definida en la ficha de aplicaciones de intranet del PC cliente. El cliente Citrix Secure Access examina todos los paquetes transmitidos desde el dispositivo del usuario y compara las direcciones de los paquetes con la lista de aplicaciones de intranet (tabla de enrutamiento creada cuando se inició la conexión VPN). Si la dirección de destino del paquete se encuentra dentro de una de las aplicaciones de la intranet, el cliente Citrix Secure Access envía el paquete a través del túnel VPN a NetScaler Gateway. Si la dirección de destino no se encuentra en una aplicación de intranet definida, el paquete no se cifra y el dispositivo del usuario enruta el paquete de forma adecuada mediante la redirección predeterminada definida originalmente en el equipo cliente. "Cuando habilita la tunelización dividida, las aplicaciones de intranet definen el tráfico de red que se intercepta y se envía a través del túnel".

Túnel dividido inverso

NetScaler Gateway también admite la tunelización dividida inversa, que define el tráfico de red que NetScaler Gateway no intercepta. Si establece la tunelización dividida como inversa, las aplicaciones de intranet definen el tráfico de red que NetScaler Gateway no intercepta. Cuando habilita la tunelización dividida inversa, todo el tráfico de red dirigido a direcciones IP internas omite el túnel VPN, mientras que el resto del tráfico pasa por NetScaler Gateway. La tunelización dividida inversa se puede utilizar para registrar todo el tráfico LAN no local. Por ejemplo, si los usuarios tienen una red inalámbrica doméstica y han iniciado sesión con el cliente Citrix Secure Access, NetScaler Gateway no intercepta el tráfico de red destinado a una impresora u otro dispositivo de la red inalámbrica.

> **Nota:**
>
> El cliente Citrix Secure Access para Windows también admite el túnel de división inversa basado en FQDN a partir de la versión 22.6.1.5 y versiones posteriores de Citrix Secure Access.

Puntos que tener en cuenta Tunelización dividida inversa basada en IP:

- El número de reglas basadas en direcciones IP está limitado a 1024.
- Compatible con los controladores DNE y WFP.

Tunelización dividida inversa basada en el nombre del host:

- La cantidad de nombres de host a los que se puede acceder durante una sesión de VPN está restringida por la cantidad de direcciones IP utilizables especificadas en el intervalo de suplantación de FQDN. Esto se debe a que cada nombre de host ocupa una dirección IP del intervalo de suplantación de FQDN. Una vez agotado el intervalo de direcciones IP, la dirección IP asignada menos recientemente se reutiliza para el siguiente nombre de host nuevo.
- Los sufijos DNS deben estar configurados.

  > **Nota:**
  >
  > Para los clientes de Windows, la tunelización dividida inversa basada en el nombre del host solo se admite con el controlador WFP. Habilite el modo de controlador WFP configurando el valor de registro "EnableWFP"en `1`. Para obtener más información, consulte Cliente Citrix Secure Access para Windows que utiliza la plataforma de filtrado de Windows.

Tunelización dividida inversa basada en IP y en nombres de host:

- Compatible únicamente con el controlador WFP. Se aplican todas las demás pautas mencionadas en la tunelización dividida inversa basada en IP y la tunelización dividida inversa basada en nombres de host.

Configurar resolución de servicios de nombres

Durante la instalación de NetScaler Gateway, puede utilizar el asistente de NetScaler Gateway para configurar otras opciones, incluidos los proveedores de servicios de nombres. Los proveedores de servicios de nombres traducen el nombre de dominio completo (FQDN) en una dirección IP. En el asistente de NetScaler Gateway, también puede realizar lo siguiente:

- Configurar un servidor DNS o WINS
- Establecer la prioridad de la búsqueda de DNS
- Defina el número de veces que se debe volver a intentar la conexión con el servidor.

Al ejecutar el asistente de NetScaler Gateway, puede agregar un servidor DNS. Puede agregar otros servidores DNS y un servidor WINS a NetScaler Gateway mediante un perfil de sesión. A continuación, puede indicar a los usuarios y grupos que se conecten a un servidor de resolución de nombres distinto del que utilizó originalmente el asistente para configurar.

Antes de configurar otro servidor DNS en NetScaler Gateway, cree un servidor virtual que actúe como servidor DNS para la resolución de nombres.

Para agregar un servidor DNS o WINS dentro de un perfil de sesión

1. En la utilidad de configuración, ficha de configuración > **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en Abrir.
3. En la ficha Configuración de red, realice una de las siguientes acciones:
    - Para configurar un servidor DNS, junto a Servidor **virtual DNS** , haga clic en **Anular global** , seleccione el servidor y, a continuación, haga clic **en**Aceptar .
    - Para configurar un servidor WINS, junto a **IP del servidor WINS** , haga clic en **Anular global** , escriba la dirección IP y, a continuación, haga clic **en**Aceptar .

Referencias

- Túneles divididos
- Cómo se conectan los usuarios con el cliente Citrix Secure Access
- Acerca de NetScaler Gateway
- Seleccione el método de acceso de usuario

Seleccione el método de acceso de usuario

January 26, 2024

Puede configurar NetScaler Gateway para que proporcione conexiones de usuario en los siguientes casos:

- Conexiones de usuario mediante la aplicación Citrix Workspace. La aplicación Citrix Workspace es compatible con StoreFront o la Interfaz Web para proporcionar a los usuarios acceso a aplicaciones publicadas o escritorios virtuales de un conjunto de servidores. La aplicación Citrix Workspace es un software que utiliza el protocolo de red ICA para establecer conexiones de usuario. Los usuarios instalan la aplicación Citrix Workspace en el dispositivo del usuario. Cuando los usuarios instalan la aplicación Citrix Workspace en su equipo basado en Windows o Mac, la aplicación Citrix Workspace incluye todos los complementos, incluido el cliente Citrix Secure Access para las conexiones de los usuarios. NetScaler Gateway también admite conexiones desde la aplicación Citrix Workspace para Android y la aplicación Citrix Workspace para iOS. Los usuarios pueden conectarse a sus escritorios virtuales y aplicaciones basadas en Windows, web, móviles y SaaS a través de Citrix Endpoint Management, StoreFront o la Interfaz Web.
- Conexiones de usuario con Secure Hub. Los usuarios pueden conectarse a aplicaciones móviles, web y SaaS configuradas en Endpoint Management. Los usuarios instalan Secure Hub en su dispositivo móvil (Android o iOS). Cuando los usuarios inician sesión en Secure Hub, pueden instalar WorxMail y WorxWeb, junto con cualquier otra aplicación móvil que haya instalado en Endpoint Management. Secure Hub, Secure Mail y WorxWeb utilizan la tecnología Micro VPN para establecer conexiones a través de NetScaler Gateway.
- Conexiones de usuario mediante el cliente Citrix Secure Access como aplicación independiente. El cliente Citrix Secure Access es un software que los usuarios pueden descargar e instalar en un dispositivo de usuario. Cuando los usuarios inician sesión con el complemento, los usuarios pueden acceder a los recursos de la red segura como si estuvieran en la oficina. Los recursos incluyen servidores de correo electrónico, recursos compartidos de archivos y sitios web de intranet.
- Conexiones de usuario mediante acceso sin cliente. El acceso sin cliente proporciona a los usuarios el acceso que necesitan sin necesidad de instalar software, como el cliente Citrix Secure Access o la aplicación Citrix Workspace, en el dispositivo del usuario. El acceso sin cliente permite conexiones a un conjunto limitado de recursos web, como Outlook Web Access o SharePoint, aplicaciones publicadas en Citrix Virtual Apps, escritorios virtuales de Citrix Virtual Apps and Desktops y recursos compartidos de archivos en la red segura a través de la interfaz de acceso. Los usuarios se conectan introduciendo la dirección web de NetScaler Gateway en un explorador web y, a continuación, seleccionan el acceso sin cliente en la página de opciones.

- Conexiones de usuario si se produce un error en el análisis de autenticación previa o posterior a la autenticación. Este caso se denomina respaldo del caso de acceso. El escenario alternativo de acceso permite que un dispositivo de usuario pase del cliente Citrix Secure Access a StoreFront o a la Interfaz Web, mediante la aplicación Citrix Workspace, si el dispositivo del usuario no supera el análisis inicial de endpoint.

  Si los usuarios inician sesión en NetScaler Gateway a través de la aplicación Citrix Workspace, el análisis de autenticación previa no funciona. Los análisis posteriores a la autenticación funcionan cuando NetScaler Gateway establece el túnel VPN.

Los usuarios pueden descargar e instalar el cliente Citrix Secure Access mediante los siguientes métodos:

- Conexión a NetScaler Gateway mediante un explorador web.
- Conexión a StoreFront configurada para aceptar conexiones de NetScaler Gateway.
- Instalación del complemento mediante un objeto de directiva de grupo (GPO).
- Carga del complemento NetScaler en Merchandising Server.

Implemente el cliente Citrix Secure Access para el acceso de los usuarios

January 26, 2024

NetScaler Gateway incluye los siguientes complementos para el acceso de los usuarios:

- Cliente Citrix Secure Access para Windows
- Cliente Citrix Secure Access para Mac

Cuando los usuarios inician sesión en NetScaler Gateway por primera vez, descargan e instalan el cliente Citrix Secure Access desde una página web. Los usuarios inician sesión haciendo clic en el icono de NetScaler Gateway del área de notificación de un equipo basado en Windows. En un equipo macOS X, los usuarios pueden iniciar sesión desde el **Dock o el menú Aplicaciones**. Si actualiza NetScaler Gateway a una nueva versión de software, el cliente Citrix Secure Access se actualiza automáticamente en el dispositivo del usuario.

Implemente el cliente Citrix Secure Access mediante el paquete de instalación MSI

Puede implementar el cliente Citrix Secure Access mediante una infraestructura de Microsoft Active Directory o una herramienta de implementación MSI estándar de terceros, como Windows Server Update Services. Si utiliza una herramienta compatible con paquetes de Windows Installer, puede

implementar los paquetes con cualquier herramienta que admita archivos MSI. A continuación, utiliza la herramienta de implementación para implementar e instalar el software en los dispositivos de usuario adecuados.

Ventajas de utilizar una herramienta de implementación centralizada

- Cumplimiento con los requisitos de seguridad. Por ejemplo, puede instalar software de usuario sin habilitar los privilegios de instalación de software para usuarios no administrativos.
- Control de versiones de software. Puede implementar una versión actualizada del software para todos los usuarios de forma simultánea.
- Escalabilidad. Una estrategia de implementación centralizada se escala fácilmente para dar soporte a más usuarios.
- Experiencia de usuario positiva. Puede implementar, probar y solucionar problemas relacionados con la instalación sin involucrar a los usuarios en este proceso.

Citrix recomienda esta opción cuando se prefiere el control administrativo sobre la instalación del software de usuario y el acceso a los dispositivos del usuario está disponible fácilmente.

Para obtener más información, consulte Implementación del cliente Citrix Secure Access desde Active Directory.

Determinar qué plug-in de software se va a implementar

Si la implementación de NetScaler Gateway no requiere ningún complemento de software en los dispositivos de usuario, se considera que la implementación proporciona acceso sin cliente. En este caso, los usuarios solo necesitan un explorador Web para tener acceso a los recursos de red. Sin embargo, ciertas funciones requieren el software del complemento en el dispositivo del usuario.

Seleccione el cliente Citrix Secure Access para usuarios

March 27, 2024

Al configurar NetScaler Gateway, puede elegir cómo inician sesión los usuarios. Los usuarios pueden iniciar sesión con uno de los siguientes plug-ins:

- Cliente Citrix Secure Access para Windows
- Cliente Citrix Secure Access para macOS

Para completar la configuración, cree una directiva de sesión y, a continuación, vincular la directiva a usuarios, grupos o servidores virtuales. También puede habilitar plug-ins configurando los ajustes

globales. En el perfil global o de sesión, seleccione Windows o macOS X como el tipo de plug-in. Cuando los usuarios inician sesión, reciben el plug-in tal y como se define globalmente o en el perfil y la directiva de la sesión. Cree perfiles independientes para el tipo de plug-in.

Configurar el plug-in globalmente

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, junto a Tipo de plug-in, seleccione Windows/macOS X y, a continuación, haga clic en Aceptar.

Configurar el tipo de plug-in para Windows o macOS en un perfil de sesión

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway > Directivas**y, a continuación, haga clic en Sesión.**
2. Lleve a cabo una de las siguientes acciones:
   - Si piensa crear una directiva de sesión, en el panel de detalles, haga clic en **Agregar**.
   - Si va a cambiar una directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. Cree un perfil o modifique un perfil existente. Para hacerlo, realice una de las siguientes acciones:
   - Junto a **Solicitar perfil**, haga clic en **Nuevo**.
   - Junto a **Solicitar perfil** , haz clic en **Modificar** .
4. En la ficha **Experiencia del cliente**, junto a **Tipo de plug-in**, haga clic en **Supeditación global** y, a continuación, seleccione **Windows/macOS X**.
5. Lleve a cabo una de las siguientes acciones:
   - Si piensa crear un perfil, haga clic en **Crear**, defina la expresión en el cuadro de diálogo de la directiva, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
   - Si está modificando un perfil existente, después de realizar la selección, pulse Aceptar dos veces.

Cliente Citrix Secure Access para Windows

Cuando los usuarios inician sesión en NetScaler Gateway, descargan e instalan el cliente Citrix Secure Access en el dispositivo del usuario.

Para instalar el plug-in, los usuarios deben ser administradores locales o miembros del grupo Administradores. Esta restricción se aplica únicamente a la primera instalación. Las actualizaciones de plug-ins no requieren acceso de nivel de administrador.

Para permitir que los usuarios se conecten y utilicen NetScaler Gateway, debe proporcionarles la siguiente información:

- Dirección web de NetScaler Gateway, como https://NetScalerGatewayFQDN/
- Cualquier requisito del sistema para ejecutar el cliente Citrix Secure Access si configuró los recursos y las directivas de los terminales

En función de la configuración del dispositivo de usuario, es posible que también deba proporcionar la siguiente información:

- Si los usuarios ejecutan un firewall en su equipo, deben cambiar la configuración del firewall para que el firewall no bloquee el tráfico hacia o desde las direcciones IP correspondientes a los recursos para los que ha concedido acceso. El cliente Citrix Secure Access gestiona automáticamente el Firewall de conexión a Internet en Windows XP y el Firewall de Windows en Windows XP Service Pack 2, Windows Vista, Windows 7, Windows 8 o Windows 8.1.
- Los usuarios que deseen enviar tráfico a FTP a través de una conexión de NetScaler Gateway deben configurar su aplicación FTP para que realice transferencias pasivas. Una transferencia pasiva significa que el equipo remoto establece la conexión de datos con el servidor FTP, en lugar de que el servidor FTP establezca la conexión de datos con el equipo remoto.
- Los usuarios que quieran ejecutar X aplicaciones cliente en la conexión deben ejecutar un servidor X, por ejemplo, `XManager`, en sus equipos.
- Los usuarios que instalen Receiver para Windows o Receiver para Mac pueden iniciar el cliente Citrix Secure Access desde Receiver o mediante un explorador web. Proporcione instrucciones a los usuarios sobre cómo iniciar sesión en el cliente Citrix Secure Access a través de Receiver o un explorador web.

Dado que los usuarios trabajan con archivos y aplicaciones como si fueran locales de la red de la organización, no es necesario volver a entrenar a los usuarios ni configurar aplicaciones.

Para establecer una conexión segura por primera vez, inicie sesión en NetScaler Gateway mediante la página de inicio de sesión web. El formato típico de una dirección web es.https://companyname.com Cuando los usuarios inician sesión, pueden descargar e instalar el cliente Citrix Secure Access en su equipo.

Instale el cliente Citrix Secure Access para Windows

1. En un explorador web, escriba la dirección web de NetScaler Gateway.
2. Escriba el nombre de usuario y la contraseña y, a continuación, haga clic en Inicio de sesión.
3. Seleccione Acceso a red y, a continuación, haga clic en Descargar.

4. Siga las instrucciones para instalar el plug-in.

Cuando finalice la descarga, el cliente Citrix Secure Access se conecta y muestra un mensaje en el área de notificación de un equipo con Windows.

Si desea que los usuarios se conecten al cliente Citrix Secure Access sin utilizar un explorador web, puede configurar el complemento para que muestre el cuadro de diálogo de inicio de sesión cuando los usuarios hagan clic con el botón derecho en el icono de **NetScaler Gateway** en el área de notificación de un equipo con Windows o inicien el complemento desde el menú Inicio.

Configurar el cuadro de diálogo de inicio de sesión del cliente Citrix Secure Access para Windows

Para configurar el cliente Citrix Secure Access para que utilice el cuadro de diálogo de inicio de sesión, los usuarios deben iniciar sesión para completar este procedimiento.

1. En un equipo con Windows, en el área de notificación, haga clic con el botón secundario en el icono de NetScaler Gateway y, a continuación, haga clic en Configurar NetScaler Gateway.
2. Haga clic en la ficha Perfil y, a continuación, haga clic en Cambiar perfil.
3. En la ficha Opciones, haga clic en Usar el cliente Citrix Secure Access para iniciar sesión.
   Nota: Si los usuarios abren el cuadro de diálogo
   Configurar NetScaler Gateway desde Receiver, la ficha
   Opciones no está disponible.

Configure el modo de intercepción para el cliente Citrix Secure Access para Windows

Si está configurando el cliente Citrix Secure Access para Windows, también debe configurar el modo de intercepción y configurarlo como transparente.

1. En la utilidad de configuración, haga clic en la ficha Configuración, expanda **NetScaler Gateway > Recursos y,** a continuación, haga clic en **Aplicaciones de intranet**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Pulse en **Transparente**.
5. En **Protocolo**, selecciona **CUALQUIERA**.
6. En **Tipo de destino**, seleccione **Dirección IP y máscara de red**.
7. En **dirección IP**, escriba la dirección IP.
8. En Máscara de **red, escriba la máscara**de subred, haga clic en **Crear y,** a continuación, haga clic en **Cerrar**.

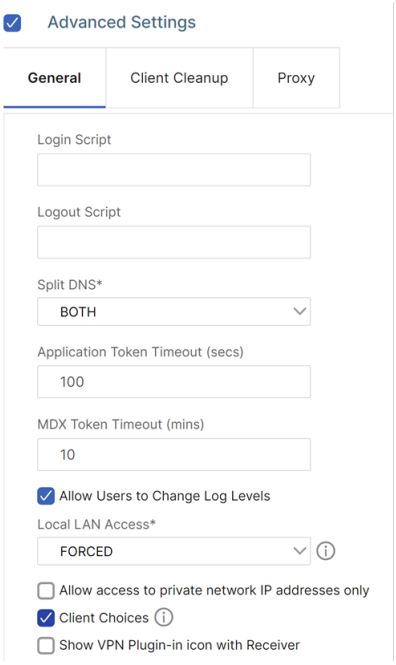
Aplique el acceso LAN local a los usuarios finales en función de la configuración de ADC

Los administradores pueden impedir que los usuarios finales inhabiliten la opción de acceso LAN local en sus máquinas cliente. Se agrega una nueva opción, FORCED a los valores de los parámetros de acceso LAN local existentes. Cuando el valor de acceso LAN local se establece en FORCED, el acceso LAN local siempre está habilitado para los usuarios finales en las máquinas cliente. Los usuarios finales no pueden inhabilitar la configuración de la LAN local mediante la interfaz de usuario del cliente de Citrix Secure Access.

Los administradores pueden permitir que los usuarios finales accedan a los recursos LAN locales de su máquina cliente configurando el parámetro de acceso LAN local en ON. Para impedir que los usuarios finales accedan a los recursos de la LAN local de su máquina cliente, los administradores pueden configurar el parámetro de acceso a la LAN local en DESACTIVADO. Para obtener más información sobre las configuraciones del usuario final, consulte Acceso LAN local para macOS y Acceso LAN local para iOS.

Para habilitar la opción Forzado mediante la GUI:

1. Vaya a **NetScaler Gateway > Configuración global > Cambiar configuración global**.
2. Haga clic en la ficha **Experiencia del cliente** y, a continuación, en **Configuración avanzada**.
3. En **Acceso LAN local**, seleccione **FORZADO**.



Para habilitar la opción Forzado mediante la CLI, ejecute el siguiente comando:

```
set vpn parameter -localLanAccess FORCED
<!--NeedCopy-->
```


Notas:

- El cliente Citrix Secure Access para macOS/iOS y las versiones posteriores admiten la funcionalidad de acceso LAN local de NetScaler Gateway.
- A partir del cliente Citrix Secure Access para Windows 23.10.1.7, el acceso LAN local se admite en un túnel a nivel de máquina si el parámetro Acceso LAN local está establecido en **Forzado** en NetScaler Gateway.

Compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows: Tech Preview

La compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows presenta una experiencia de usuario final mejorada. Para obtener más información, consulte Compatibilidad con Microsoft Edge WebView para Citrix Secure Access de Windows.

Cliente Citrix Secure Access para Windows que utiliza la plataforma de filtrado de Windows

La Plataforma de filtrado de Windows (WFP) es un conjunto de servicios de API y sistema que proporciona una plataforma para crear aplicaciones de filtrado de red. WFP está diseñado para reemplazar las tecnologías de filtrado de paquetes anteriores, el filtro de especificación de interfaz de controlador de red (NDIS) que se utilizaba con el controlador DNE. El modo WFP es compatible con la versión 22.6.1.5 del cliente Citrix Secure Access para Windows.

Instalar la compilación de WFP

Puede instalar la compilación de WFP mediante uno de los métodos siguientes.

- Instalar el plug-in VPN con los controladores DNE y WFP (método predeterminado)

  Cuando el plug-in se instala con los controladores DNE y WFP, los administradores pueden usar el controlador WFP o DNE para tunelizar a través de un botón del Registro. De forma predeterminada, el controlador DNE se usa para la tunelización.

- Instale el plug-in VPN solo con el controlador WFP (omita la instalación del controlador DNE)

  Los controladores DNE no son compatibles con algunas de las aplicaciones de terceros, incluso cuando no se usan. Para esas implementaciones, los administradores pueden usar este tipo de instalación. Como el controlador DNE no está instalado, solo se utiliza el controlador WFP para la tunelización.

Seleccione un controlador WFP en lugar de un controlador DNE

Siga estos pasos para seleccionar el controlador WFP en lugar del controlador DNE.

> **Nota:**
>
> Esto solo funciona con el método de instalación predeterminado.

1. Descargue la compilación del plug-in VPN compatible con WFP e instale el nuevo plug-in VPN.
2. De forma predeterminada, el controlador DNE se usa para tunelizar el tráfico. Para usar el controlador de WFP para la tunelización, los administradores deben crear la siguiente entrada del Registro:
   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE —Establece el valor en 1 para usar WFP y 0 para usar DNE (de forma predeterminada, DNE está habilitado si este valor del Registro no está presente o se establece en 0)

> **Nota:**
>
> Después de cambiar el modo de tunelización de DNE a WFP o viceversa, se debe reiniciar el sistema para que los cambios surtan efecto correctamente.

Omitir por completo la instalación de DNE

Siga estos pasos para omitir la instalación de DNE.

1. Realice una desinstalación limpia del plug-in VPN.
   a) Desinstale el plug-in VPN actual presente en el equipo y reinícielo.
   b) Compruebe si el controlador DNE se ha desinstalado mediante cualquiera de las siguientes opciones.
      - Abra un símbolo del sistema con privilegios elevados (o PowerShell). Ejecute los siguientes comandos (el resultado de ejemplo muestra que el controlador basado en DNE está instalado en el sistema)

```
PS C:\Users\Administrator> sc qc cag
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: cag
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 2   AUTO_START
ERROR_CONTROL      : 1   NORMAL
```



```
BINARY_PATH_NAME   : ??\C:\Program Files\Common Files\
    Deterministic Networks\Common Files\cag.sys
LOAD_ORDER_GROUP   :
TAG                : 0
DISPLAY_NAME       : Citrix cag plugin for Access Gateway
DEPENDENCIES       :
SERVICE_START_NAME :
PS C:\Users\Administrator> sc qc dne
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dne
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 1   SYSTEM_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys
LOAD_ORDER_GROUP   : NDIS
TAG                : 38
DISPLAY_NAME       : DNE LightWeight Filter
DEPENDENCIES       :
SERVICE_START_NAME :
<!--NeedCopy-->
```

Si el controlador no está instalado, se muestra el siguiente resultado:

```
The specified service does not exist as an installed service.
```

Dado que otros proveedores también utilizan el controlador DNE (dnelwf64.sys), es posible que esté presente incluso cuando el cliente Citrix Secure Access no esté instalado en el sistema. Por otro lado, el complemento CAG solo lo usa el cliente Citrix Secure Access.

- La presencia del DNE también se puede comprobar intentando iniciar los controladores CAG y DNE. Abra el símbolo del sistema con derechos de administrador y ejecute los siguientes comandos:

```
net start cag
net start dne
<!--NeedCopy-->
```

  - Si el mensaje de salida indica que no se pueden encontrar los servicios (el nombre del servicio no es válido), el plug-in y los componentes del controlador se desinstalarán correctamente. En este caso, vaya al paso 2.
  - Si los componentes del plug-in y el controlador no se desinstalan correctamente, ejecute la utilidad Cleanup en el equipo cliente siguiendo las instrucciones que se proporcionan en.https://citrix.sharefile.com/d-s829800c3821a4a8f869ad324de6f0332
    * Descomprima la utilidad Cleanup y cópiela en una carpeta.
    * Ejecute nsRmSAC.exe desde el símbolo del sistema.
    * Reinicie la máquina cliente.

2. Cree las siguientes entradas del Registro.

- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - SkipDNE
  - REG_VALUE - Establézcala en 1 para asegurarse de que el DNE no esté instalado en la máquina
- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - EnableWFP
  - REG_VALUE - Establézcala en 1 para habilitar WFP (esta entrada debe crearse si se omite la instalación de DNE)

> **Nota:**
>
> - Si las entradas del Registro no se crean antes de la instalación, se instala DNE de forma predeterminada. Además, puede comprobar los archivos de registro de VPN para validar si se utiliza WFP o DNE.
> - Si se omite la instalación de DNE, EnableWFP debe establecerse en 1. En este caso, no puede cambiar al complemento basado en DNE sin volver a instalar el cliente Citrix Secure Access.

3. Instale el nuevo plug-in de VPN.
4. Confirme si el controlador de WFP está instalado en el sistema. Abra un símbolo del sistema con privilegios elevados y ejecute el siguiente comando. El resultado de ejemplo muestra que el controlador de WFP está instalado en el sistema.

```
PS C:\Users\Administrator> sc qc ctxsgwcallout
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ctxsgwcallout
    TYPE               : 1  KERNEL_DRIVER
    START_TYPE         : 1   SYSTEM_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : ??\C:\Program Files\Citrix\Secure Access
       Client\ctxsgwcallout.sys
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Citrix Secure Access Callout Driver
    DEPENDENCIES       :
    SERVICE_START_NAME :
<!--NeedCopy-->
```

Si el controlador no está instalado, se muestra el siguiente resultado:

```
The specified service does not exist as an installed service.
```

1. Reinicie la máquina cliente.

Ventajas de WFP

Las siguientes son algunas de las ventajas de WFP si se realiza la instalación independiente del controlador de WFP en el cliente.

- **Compatibilidad con túnel dividido inverso basado en FQDN:** El controlador de WFP permite la compatibilidad con túneles divididos INVERSOS basados en FQDN. No se admite con el controlador DNE. Para obtener más información, consulte Opciones de tunelización dividida.
- **Compatibilidad con Wireshark:** DNE no permite capturar tráfico bidireccional en una máquina cliente debido a su vinculación con el adaptador Ethernet/Wi-Fi. Este no es un problema con el nuevo controlador de WFP. Cualquier captura de tráfico (unidireccional o bidireccional) está cifrada y requiere claves SSL para descifrarla.
- **Compatibilidad con NMAP:** El nuevo controlador WFP admite el escaneo de NMAP mientras que el complemento VPN se utiliza para tunelizar el tráfico, mientras que el DNE no permite el escaneo de NMAP, mientras que el complemento de VPN se utiliza para tunelizar el tráfico.
- **Velocidad de la red:** En algunos casos, si el DNE está instalado en un equipo cliente, la velocidad de descarga y carga se ve afectada, lo que no ocurre con WFP.
- **Rendimiento mejorado de nslookup:** A veces, con DNE, `nslookup`no responde con un número menor de intentos y no se observa lo mismo con WFP.
- **Rendimiento mejorado de iperf sobre UDP:** Con DNE, se observó cierta pérdida de paquetes durante las pruebas de escalabilidad con iperf sobre UDP. La pérdida de paquetes no se observa con WFP.

Implemente el cliente Citrix Secure Access desde Active Directory

January 26, 2024

Si los usuarios no tienen privilegios administrativos para instalar el cliente Citrix Secure Access en el dispositivo del usuario, puede implementar el complemento para los usuarios desde Active Directory. Al utilizar este método para implementar el cliente Citrix Secure Access, puede extraer el programa de instalación y, a continuación, utilizar una directiva de grupo para implementar el programa. Los pasos generales para este tipo de implementación son los siguientes:

- Extracción del paquete MSI.
- Distribución del plug-in mediante una directiva de grupo.
- Creación de un punto de distribución.

- Asignación del paquete de cliente Citrix Secure Access mediante un objeto de directiva de grupo.

  Nota: La distribución del cliente Citrix Secure Access desde Active Directory solo se admite en Windows 7, Windows 8 y Windows 10.

Puede descargar el paquete MSI desde la utilidad de configuración o desde el sitio web de Citrix.

Para descargar el paquete MSI del cliente Citrix Secure Access desde la utilidad de configuración

1. En la utilidad de configuración, haga clic en **Descargas**.
2. En el cliente Citrix Secure Access, haga clic en **Descargar el complemento NetScaler Gateway para Windows** y, a continuación, guarde el archivo **nsvpnc_setup.exe** en su servidor de Windows.

   Nota:

   - Para equipos de 64 bits, debe guardar el archivo Agee_setup.exe en el servidor Windows.
   - Si no aparece el cuadro de diálogo **Descarga de archivos**, pulse la tecla CTRL al hacer clic en el enlace **Descargar el cliente Citrix Secure Access para Windows**.

3. En el símbolo del sistema, vaya a la carpeta en la que guardó **nsvpnc_setup.exe** y, a continuación, escriba:

   ```
   nsvpnc_setup /c
   <!--NeedCopy-->
   ```

   Esto extrae el archivo agee.msi.

   Nota: Para equipos de 64 bits, vaya a la carpeta en la que guardó **Agee_setup.exe** y, a continuación, escriba:

   ```
   Agee_setup.exe /c
   <!--NeedCopy-->
   ```

   Esto extrae el archivo agee64.msi.

4. Guarde el archivo extraído en una carpeta del servidor Windows.

Después de extraer el archivo, utilice una directiva de grupo en Windows Server para distribuirlo.

Antes de iniciar la distribución, instale la Consola de administración de directivas de grupo en Windows Server 2003, Windows Server 2008 o Windows Server 2012. Para obtener más información, consulte la ayuda en línea de Windows.

Nota: Al utilizar una directiva de grupo para publicar el cliente Citrix Secure Access, Citrix recomienda asignar el paquete al dispositivo del usuario. El paquete MSI se instala por dispositivo.

Antes de poder distribuir el software, cree un punto de distribución en un recurso compartido de red de un servidor de publicación, como Microsoft Internet Security and Acceleration (ISA) Server.

Para crear un punto de distribución

1. Inicie sesión en el servidor de publicación como administrador.
2. Cree una carpeta y compártala en la red con permiso de lectura para todas las cuentas que necesiten acceso al paquete de distribución.
3. En el símbolo del sistema, vaya a la carpeta en la que guarde el archivo extraído y, a continuación, escriba: msiexec -a agee.msi
4. En la pantalla **Ubicación de red**, haga clic en **Cambiar** y, a continuación, vaya a la carpeta compartida en la que desee crear la instalación administrativa del cliente Citrix Secure Access.
5. Haga clic en **Aceptar** y luego en **Instalar**.

Después de colocar el paquete extraído en el recurso compartido de red, asigne el paquete a un objeto de directiva de grupo en Windows.

Tras configurar correctamente el cliente Citrix Secure Access como paquete de software administrado, el complemento se instalará automáticamente la próxima vez que se inicie el dispositivo del usuario.

> **Nota:** Cuando el paquete de instalación se asigna a un equipo, el usuario debe reiniciarlo.

Cuando se inicia la instalación, los usuarios reciben un mensaje que indica que el cliente Citrix Secure Access se está instalando.

Administre el cliente Citrix Secure Access mediante Active Directory

January 26, 2024

Cada versión del cliente Citrix Secure Access se empaqueta como una instalación completa del producto, en lugar de como un parche. Cuando los usuarios inician sesión y el cliente Citrix Secure Access detecta una nueva versión del complemento, el complemento se actualiza automáticamente. También puede implementar el cliente Citrix Secure Access para actualizarlo mediante Active Directory.

Para ello, cree un punto de distribución para el cliente Citrix Secure Access. Cree un objeto de directiva de grupo y asígnele la nueva versión del complemento. A continuación, cree un vínculo entre el nuevo paquete y el paquete existente. Tras crear el enlace, se actualiza el cliente Citrix Secure Access.

Eliminar el cliente Citrix Secure Access de los dispositivos de usuario

Para eliminar el cliente Citrix Secure Access de los dispositivos de usuario, elimine el paquete asignado del Editor de objetos de directiva de grupo.

Cuando se quita el complemento del dispositivo del usuario, los usuarios reciben un mensaje que indica que el complemento se está desinstalando.

Solucionar problemas de instalación del cliente Citrix Secure Access mediante Active Directory

Si el paquete asignado no se instala cuando se inicia el dispositivo del usuario, es posible que aparezca la siguiente advertencia en el registro de sucesos de la aplicación:

No se han podido aplicar los cambios a la configuración de instalación del software. La aplicación de directivas de instalación de software se ha retrasado hasta el siguiente inicio de sesión porque un administrador ha habilitado la optimización de inicios de sesión para la directiva de grupo. El error fue: El marco de directivas de grupo debe llamar a la extensión en la actualización sincrónica de la directiva de primer plano.

Este error se debe a la optimización de inicio de sesión rápido en Windows XP, en la que los usuarios pueden iniciar sesión antes de que el sistema operativo inicialice todos los componentes de red, incluido el procesamiento de objetos de directiva de grupo. Algunas directivas pueden requerir más de un reinicio para que surtan efecto. Para resolver este problema, inhabilite la optimización de inicio de sesión rápido en Active Directory.

Para solucionar otros problemas de instalación del software administrado, Citrix recomienda utilizar una directiva de grupo para habilitar el registro de Windows Installer.

Integre el cliente Citrix Secure Access con la aplicación Citrix Workspace

January 26, 2024

NetScaler Gateway admite la aplicación Citrix Workspace. El sistema orquestado consta de los siguientes componentes:

- Aplicación Citrix Workspace para Windows 3.4 o posterior
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para Android
- Aplicación Citrix Workspace para iOS
- StoreFront 2.1 o posterior

- Endpoint Management 2.8 y versiones posteriores o Citrix Endpoint Management 10
- Citrix Update Service alojado en el sitio web de Citrix

Para obtener más información sobre la compatibilidad de NetScaler Gateway con los productos de NetScaler, consulte Compatibilidadcon los productos de NetScaler.

Puede configurar NetScaler Gateway para que, cuando los usuarios inicien sesión en el dispositivo, el cliente Citrix Secure Access abra un navegador web que permita el inicio de sesión único en la página principal de la aplicación Citrix Workspace. Los usuarios pueden descargar la aplicación Citrix Workspace desde la página principal.

Cuando los usuarios inician sesión con la aplicación Citrix Workspace, las conexiones de usuario se pueden redirigir a través de NetScaler Gateway de la siguiente manera:

- Directamente a Endpoint Management
- Directamente a StoreFront
- A StoreFront y, a continuación, a Endpoint Management si no configura las aplicaciones móviles MDX en Endpoint Management
- A Endpoint Management y luego a StoreFront si configura aplicaciones móviles MDX en Endpoint Management

> **Nota:**
>
> Las conexiones que se enrutan directamente a Endpoint Management solo son compatibles con Endpoint Management 2.0, Endpoint Management 2.5, Endpoint Management 2.6, Endpoint Management 2.8 y Endpoint Management 2.9. Si ha implementado Endpoint Management 1.1 en su red, las conexiones de usuario deben dirigirse a través de StoreFront.

Cómo se conectan los usuarios con la aplicación Citrix Workspace

January 26, 2024

Los usuarios pueden conectarse a las siguientes aplicaciones, escritorios y datos desde la aplicación Citrix Workspace:

- Aplicaciones basadas en Windows y escritorios virtuales publicados en StoreFront y en la interfaz web
- Acceso a los datos de ShareFile mediante Citrix Endpoint Management

Los usuarios pueden iniciar sesión mediante cualquiera de las siguientes aplicaciones de Citrix Workspace:

- Aplicación Citrix Workspace para Web

- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para iOS
- Aplicación Citrix Workspace para Android

Los usuarios pueden iniciar sesión con la aplicación Citrix Workspace para Web mediante un explorador web o desde el icono de la aplicación Citrix Workspace del dispositivo del usuario.

Cuando los usuarios inician sesión con cualquier versión de la aplicación Citrix Workspace, las aplicaciones, los datos de ShareFile y los escritorios aparecen en el explorador o en la ventana de la aplicación Citrix Workspace.

Desacoplar el icono de la aplicación Citrix Workspace

March 27, 2024

Cuando se configura una implementación de Citrix Virtual Apps and Desktops con el cliente Citrix Secure Access integrado en la aplicación Citrix Workspace, el usuario que esté conectado a la VPN no podrá ver el icono del complemento. El icono de **Citrix Secure Access** normalmente se encuentra en la bandeja del sistema de Windows o en la barra de menús de macOS X Finder. Este icono es la interfaz de los ajustes y controles del plug-in. Para los usuarios de Windows, cuando la aplicación Citrix Workspace y el cliente Citrix Secure Access están integrados, el cuadro de diálogo **Acerca** de la aplicación Citrix Workspace muestra los controles del cliente Citrix Secure Access. Para los usuarios de macOS X, no hay controles para el cliente Citrix Secure Access disponibles después de la integración.

Algunas implementaciones integradas pueden presentar la necesidad de exponer los controles del plug-in sin perder la integración de la funcionalidad subyacente. Para ello, utilice el siguiente comando de CLI o la tarea de la utilidad de configuración de NetScaler para alternar la integración de iconos para clientes VPN.

Establecer la integración de iconos mediante la CLI

En la línea de comandos, escriba;

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

Establecer la integración de iconos mediante la interfaz gráfica de usuario

1. En la ficha Configuración, vaya a **NetScaler Gateway > Configuración global**.

2. Haga clic en **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. Haga clic en **Configuración avanzada.**
4. Seleccione **Mostrar el icono del complemento VPN** con la aplicación Citrix Workspace.

Configuración de IPv6 para conexiones ICA

March 27, 2024

NetScaler Gateway admite direcciones IPv6 para conexiones ICA. Las conexiones con IPv6 a la interfaz web o StoreFront funcionan igual que las conexiones IPv4. Cuando los usuarios se conectan mediante la dirección web de NetScaler Gateway, NetScaler Gateway envía como proxy la conexión a la interfaz web o StoreFront.

Puede configurar IPv6 para NetScaler Gateway implementado en una DMZ o implementado en una DMZ de doble salto.

Puede habilitar IPv6 en NetScaler Gateway mediante la línea de comandos. Puede usar las siguientes pautas:

- Habilite IPv6 en el dispositivo.
- Configure las direcciones IP de subred.
- Defina el orden de resolución de DNS.
- Defina la interfaz web o la dirección web de StoreFront.
- Vincule Secure Ticket Authority (STA) a NetScaler Gateway.

De forma predeterminada, la dirección IP asignada no admite direcciones IPv6. Para redirigir las comunicaciones de los usuarios a la red interna, debe crear direcciones IP de subred y, a continuación, configurar NetScaler Gateway para que utilice las direcciones IP de subred.

Si implementa varias subredes IPv6 en la red, cree varias direcciones IP de subred IPv6 en NetScaler Gateway, para cada subred de la red. La redirección de red envía los paquetes IPv6 a las subredes respectivas mediante las direcciones IP de subred.

Para configurar IPv6 para el proxy ICA mediante la CLI

1. Inicie sesión en NetScaler Gateway mediante una conexión de Secure Shell (SSH), como desde PuTTY. En la línea de comandos, escriba;


```
enable ns feature IPv6PT. This enables IPv6.

enable ns mode USNIP.

set dns parameter  – resolutionOrder AAAAThenAQuery AThenAAAAQuery
   OnlyAAAAQuery OnlyAQuery

set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`

<!--NeedCopy-->
```

Donde es el nombre de dominio o la dirección IP de StoreFront.

Ejemplo:

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb
    `.
<!--NeedCopy-->
```

O bien

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
<!--NeedCopy-->
```

> **Nota:**
>
> Si utiliza la dirección IPv6 para configurar este parámetro, la dirección IP debe estar entre corchetes.

Configurar la página principal de la aplicación Citrix Workspace en NetScaler Gateway

March 27, 2024

Puede configurar la página principal de la aplicación Citrix Workspace de forma global o como parte de un perfil de sesión. Si quiere configurar la aplicación Citrix Workspace para Web y versiones anteriores de la aplicación Citrix Workspace que no reconocen StoreFront a través de NetScaler Gateway, debe crear dos perfiles de sesión independientes. El campo Página de inicio de la aplicación Citrix Workspace debe tener la dirección web correcta para cada perfil para que los usuarios puedan iniciar sesión correctamente.

Para las aplicaciones Citrix Workspace que reconocen StoreFront a través de NetScaler Gateway, puede hacer que la aplicación Citrix Workspace para Web y la aplicación Citrix Workspace compartan un perfil. Sin embargo, Citrix recomienda configurar un perfil de sesión para la aplicación Citrix

Workspace para Web y un perfil de sesión independiente para todas las demás aplicaciones de Citrix Workspace.

Para configurar la página principal de la aplicación Citrix Workspace de forma global

Para configurar la página principal de la aplicación Citrix Workspace de forma global:

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En el cuadro de diálogo Configuración global de NetScaler Gateway, haga clic en la ficha Aplicaciones publicadas.
4. En la página principal de la aplicación Citrix Workspace, escriba la dirección web de la aplicación Citrix Workspace o la página de inicio de la aplicación Citrix Workspace para Web y, a continuación, haga clic en Aceptar.

Para configurar la página principal de la aplicación Citrix Workspace en un perfil de sesión

Para configurar la página principal de la aplicación Citrix Workspace en un perfil de sesión:

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway > Directivas**y, a continuación, haga clic en Sesión.**
2. En el panel de detalles, en la pestaña **Perfiles** , haga clic en **Agregar** .
3. En el cuadro de diálogo **Crear perfil de sesión de NetScaler Gateway**, en la ficha **Aplicación publicada**, junto a la Página **inicial de Citrix Receiver**, haga clic en **Supedición global**.
4. En la página principal de la aplicación Citrix Workspace, escriba la dirección web de la página principal de la aplicación Citrix Workspace o de la aplicación Citrix Workspace para Web y, a continuación, haga clic en **Crear**.

Aplicar el tema de la aplicación Citrix Workspace a la página de inicio de sesión de NetScaler Gateway

March 27, 2024

Puede usar la interfaz de usuario de NetScaler Gateway para aplicar el tema de la aplicación Citrix Workspace a la página de inicio de sesión de NetScaler Gateway. Puede cambiar entre el tema de la aplicación Citrix Workspace y el tema personalizado que cree. Una vez creado el tema personalizado, borre la memoria caché del explorador web para evitar que aparezcan páginas almacenadas en caché.

De forma predeterminada, la página de inicio de sesión de NetScaler Gateway usa el tema visual RfWebUI que coincide con el estilo de la interfaz de usuario unificada que usa StoreFront. Si utiliza la plataforma Citrix Workspace o StoreFront local con la nueva interfaz de usuario de Workspace, siga las instrucciones que se proporcionan en este artículo de asistencia. También puede crear su propio tema personalizado. Para obtener más información, consulte Crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway.

Asegúrese de que el tema del portal de NetScaler Gateway esté enlazado a un servidor virtual VPN. Para obtener más información, consulte Vincular un tema de portal a un servidor virtual VPN.

Crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway

January 26, 2024

Puede utilizar la interfaz gráfica de usuario para crear un tema personalizado para la página de inicio de sesión de NetScaler Gateway. También puede dejar el tema predeterminado o usar el tema de la aplicación Citrix Workspace. Cuando elige aplicar un tema personalizado a la página de inicio de sesión, utiliza la línea de comandos de NetScaler Gateway para crear e implementar el tema. A continuación, utilice la interfaz gráfica de usuario para configurar la página del tema personalizado.

La página de temas personalizados se configura mediante la configuración global de NetScaler Gateway.

Puede utilizar esta función con las siguientes versiones de NetScaler Gateway:

- NetScaler Gateway 10.1
- Access Gateway 10, compilación 73.5002.e (debe instalar esta compilación después de la compilación 71.6104.e para usar esta función con las versiones 2.5, 2.6 o 2.8 de Endpoint Management)
- Access Gateway 10, compilación 71.6104.e

Crear e implementar el tema personalizado mediante la CLI

Para crear e implementar el tema personalizado mediante la línea de comandos:

1. Inicie sesión en la línea de comandos de NetScaler Gateway.
2. En el símbolo del sistema, escriba shell.
3. En el símbolo del sistema, escriba `mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*`.
4. Utilice la utilidad de configuración para cambiar al tema personalizado y, a continuación, realizar cambios de personalización en /var/ns_gui_custom/ns_gui/vpn. Puede hacer lo siguiente:
   - Realice ediciones en el archivo css/ctx.authentication.css.
   - Copie un logotipo personalizado en la carpeta /var/ns_gui_custom/ns_gui/vpn/media. **Nota:** Puede utilizar WinSCP para transferir los archivos.
5. Si tiene varios dispositivos NetScaler Gateway, repita los pasos 3 y 4 para todos los dispositivos.

Claves de Registro del cliente VPN de Windows de NetScaler Gateway

March 27, 2024

Las claves de registro del cliente VPN están disponibles en **HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client**. En la siguiente tabla se enumeran las claves de registro del cliente VPN para Windows de NetScaler Gateway, los valores y una breve descripción de cada valor.

Clave del Registro	Tipo de Registro	Valores y descripción
addedRoutes/modifiedRoutes	REG_SZ	Creado para la comunicación interna de plug-ins. Los usuarios no deben modificar esta clave.
AlwaysOnService	REG_DWORD	1 => Establezca un túnel a nivel de máquina pero no un túnel a nivel de usuario. 2 => Establecer túnel a nivel máquina y túnel de usuario.
AlwaysOnURL	REG_SZ	URL del servidor virtual de NetScaler Gateway al que el usuario quiere conectarse. Ejemplo: *https://xyz.companyDomain.com*

Clave del Registro	Tipo de Registro	Valores y descripción
AlwaysOn	REG_DWORD	1 => Permitir acceso a la red en caso de fallo de VPN. 2=> Bloquear el acceso a la red en caso de fallo
AlwaysOnAllowlist	REG_SZ	Lista separada por puntos y comas de las direcciones IP o FQDN permitidas por el conductor en el modo estricto Always On.
ClientControl	REG_DWORD	1 => Permite a los usuarios cerrar sesión o conectarse a otras puertas de enlace. 0 => Bloquea que los usuarios cierren sesión o se conecten a otras puertas de enlace.
ConfigSize	REG_DWORD	El cliente de Windows admite un tamaño de archivo de configuración de 64 KB de forma predeterminada. Utilice este Registro para aumentar el tamaño del archivo de configuración. Si el tamaño del archivo de configuración es mayor que el valor predeterminado (64 KB), el valor del Registro ConfigSize debe establecerse en 5 x 64 KB (después de convertirlo en bytes) por cada incorporación de 64 KB. Por ejemplo, si piensa agregar 64 KB más, debe establecer el valor del Registro en 64 x 1024 x 5 = 327680. Del mismo modo, si agrega 128 KB, debe establecer el valor del Registro en 64 x 1024 x (5+5) = 655360.

Clave del Registro	Tipo de Registro	Valores y descripción
Connected	REG_DWORD	Si la conexión se realiza correctamente, esta clave se establece en 1 y en 0. Esta clave se utiliza internamente. Los usuarios no deben modificar esta clave.
DisableGA	REG_DWORD	Establezca el valor 1 para inhabilitar Google analytics.
DisableCredProv	REG_DWORD	Cuando está habilitado Siempre activado antes del inicio de sesión del usuario, el plug-in de la VPN de Windows agrega el proveedor de credenciales para mostrar el estado del túnel en la pantalla de inicio de sesión. Si no necesita esta funcionalidad adicional, cree y defina este registro en 1.
DisableIconHide	REG_DWORD	1 => La aplicación Citrix Workspace y el plug-in de puerta de enlace se muestran en la barra de tareas. 0 => El icono del plug-in de puerta de enlace está integrado en la aplicación Citrix Workspace para Windows. El complemento de puerta de enlace no está visible en la barra de tareas cuando se ejecuta una sesión de VPN completa.

Clave del Registro	Tipo de Registro	Valores y descripción
DisableDNSRoutes	REG_DWORD	Valor predeterminado 0 => El plug-in de la VPN agrega rutas para los servidores DNS si son diferentes de la puerta de enlace predeterminada de una interfaz física. Sin embargo, según la topología de la máquina cliente de Windows, es posible que las rutas del servidor DNS no siempre sean necesarias.p Si se establece en 1, el complemento VPN no agrega rutas explícitas para los servidores DNS.
DisallowCaptivePortals	REG_DWORD	1 => El plug-in de la VPN comprueba si hay portales cautivos al intentar conectarse a la página de prueba de Microsoft Connect antes de iniciar una sesión de VPN. 0 => El plug-in de la VPN omite la comprobación de los portales cautivos.
DisableIntuneDeviceEnrollment	REG_DWORD	Si se establece en 1, no se realiza la inscripción de dispositivos Intune.
EnableAutoUpdate	REG_DWORD	Se utiliza para controlar la funcionalidad de actualización de plug-ins desde el lado del cliente. Establezca en 0 para inhabilitar la funcionalidad de actualización automática. Establezca en 1 para respetar la configuración de ADC.
EnableKerberosAuth	REG_DWORD	0 => Valor predeterminado. 1 => El cliente VPN usa el método de autenticación Kerberos para el inicio de sesión automático.

Clave del Registro	Tipo de Registro	Valores y descripción
EnableVA	REG_DWORD	Si el adaptador Citrix Virtual debe estar habilitado cuando IIP está presente. Esta clave se utiliza internamente. Los usuarios no deben modificar esta clave.
EnableWFP	REG_DWORD	Valor predeterminado 0 => De forma predeterminada, DNE está activado. 1 => El plug-in de VPN usa WFP. 0 => El plug-in de VPN usa DNE.
ForcedLogging	REG_DWORD	Establezca esta clave en 1 para habilitar el registro de depuración.
HttpTimeout	REG_DWORD	El tiempo de espera HTTP se configura en segundos. Si el tiempo de espera no está configurado, se utiliza el tiempo de espera predeterminado. El valor de tiempo de espera predeterminado es de 100 segundos, según los estándares de Windows.
InstallDir	REG_SZ	Ubicación en la que está instalado el cliente Citrix Secure Access.
locationDetection	REG_DWORD	1 => Para habilitar la detección de ubicación. 0 => Para inhabilitar la detección de ubicación.
NoDHCPRoute	REG_DWORD	Si se establece en 1, no se agrega la ruta del servidor DHCP.
overrideIPV6DnsDrop	REG_DWORD	1 => Permitir que el tráfico DNS de IPv6 fluya a través de la VPN. 0 => Restringir el flujo de tráfico DNS de IPv6.

Clave del Registro	Tipo de Registro	Valores y descripción
OverrideSpoofIPRange	Necesita entradas de inglés	Detecta si hay conflictos en el rango de direcciones IP falsas predeterminado o configurado por el administrador y aplica un nuevo rango de direcciones IP falsas.
ProductVersion	REG_SZ	Versión instalada actual del cliente Citrix Secure Access.
ProductCode	REG_SZ	Esta clave se utiliza internamente. Los usuarios no deben modificar esta clave.
secureDNSUpdate	REG_DWORD	0 => El complemento de VPN solo intenta la actualización de DNS no segura. 1 => El complemento de VPN intenta primero la actualización de DNS no segura. Si la actualización de DNS no segura falla, el complemento de VPN intenta la actualización de DNS segura. Este es el comportamiento predeterminado a partir de la compilación del complemento de Windows 21.3.1.2. 2 => El plug-in de la VPN solo intenta la actualización de DNS segura.

Clave del Registro	Tipo de Registro	Valores y descripción
SecureChannelResetTimeoutSeconds	REG_DWORD	De forma predeterminada, este valor de Registro no se establece ni se agrega. Cuando el valor de "SecureChannelResetTimeoutSeconds"es 0xFFFFFFFF o no está presente en el registro, el plug-in de la VPN espera a que finalice la llamada a la API SecureChannelReset() antes de empezar a tunelizar el tráfico de datos. Este es el comportamiento predeterminado. El administrador debe configurar este registro en el cliente para que el plug-in de la VPN comience a tunelizar el tráfico de datos después de esperar el tiempo especificado para que se complete la llamada a la API.
SecureAccessLogInScript	REG_SZ	Citrix Secure Access Service accede a la configuración del script de inicio de sesión mediante esta clave de Registro cuando se conecta a Citrix Secure Private Access Service. Para obtener más información, consulte Registros de configuración de scripts de inicio y cierre de sesión.

Clave del Registro	Tipo de Registro	Valores y descripción
SecureAccessLogOutScript	REG_SZ	Citrix Secure Access Service accede a la configuración del script de cierre de sesión mediante esta clave de registro cuando se conecta a Citrix Secure Private Access Service. Para obtener más información, consulte Registros de configuración de scripts de inicio y cierre de sesión.
suffixList	REG_SZ	Lista de dominios de intranet con puntos y comas. Se utiliza cuando la detección de ubicación está habilitada.
Puerto SIC Begin	REG_DWORD	Evita los conflictos que pueden surgir al utilizar puertos para crear sockets entre el cliente Citrix Secure Access y las aplicaciones de terceros en las máquinas cliente. El rango permitido es de 49152 a 64535 (de C000 a FC17 en formato hexadecimal). El cliente VPN utiliza hasta 1000 puertos a partir de `SicBeginPort`solo si `EnableWFP`también está configurado en.1
userCertCAList	REG_SZ	Se utiliza en el contexto del servicio Always On, en el que un cliente puede especificar la lista de CA para elegir el certificado de cliente.

> **Importante:**
>
> - Puede aplicar claves de registro en función de sus implementaciones. Por ejemplo, la clave del Registro AlwaysOnService solo se aplica al servicio Always On, mientras que la clave del

> Registro ClientControl no se aplica al servicio Always On. Consulte la documentación sobre implementaciones individuales para obtener más detalles.
>
> - `secureDNSUpdate` solo se aplica a los dispositivos cliente unidos a un dominio.
> - Para el cliente de Citrix Secure Access para Windows 23.1.1.8 y versiones posteriores, el nombre de la clave de Registro es.`overrideIPV6DnsDrop` Para el cliente de Citrix Secure Access para Windows 22.10.1.9 y versiones anteriores, el nombre de la clave de Registro es.`overrideIP6DnsDrop`

Aplicar el indicador HttpOnly en las cookies de autenticación

March 27, 2024

A partir de las versiones 13.1-37.x y posteriores de NetScaler Gateway, el indicador HttpOnly está disponible en las cookies de autenticación de los casos con VPN, es decir, en las cookies NSC_AAAC y NSC_TMAS. La cookie de autenticación NSC_TMAS se usa durante la autenticación nFactor y la cookie NSC_AAAC se usa para la sesión autenticada. El indicador HttpOnly de una cookie restringe el acceso a las cookies mediante la opción de cookie de documentos de JavaScript. Esto ayuda a evitar el robo de cookie debido a las secuencias de comandos entre sitios.

Caso admitido

El indicador HttpOnly es compatible con la autenticación nFactor.

Comportamiento cuando se usa el botón HttpOnlyCookie del parámetro AAA de NetScaler junto con el botón HttpOnlyCookie de tmsession:

- Cuando el botón HttpOnlyCookie del parámetro de autenticación, autorización y auditoría está activado y se utiliza la autenticación nFactor, el botón HttpOnlyCookie del parámetro de autenticación, autorización y auditoría supedita el botón HttpOnlyCookie de la sesión TM. Además, tanto NSC_TMAS como NSC_AAAC se marcan como HttpOnly independientemente del tipo de sesión, ya sea una sesión de VPN, una sesión de TM o durante la autenticación de nFactor.
- Si el botón HttpOnlyCookie está inhabilitado, el indicador HttpOnly no está configurado para una sesión de VPN. Para el caso de autenticación, autorización y auditoría, el indicador HttpOnly se establece en función del valor del botón de sesión de TM.

Configurar la función HttpOnly mediante la CLI

- Habilitar el indicador HttpOnly


```
set aaa parameter -httpOnlyCookie ENABLED
<!--NeedCopy-->
```

- Comprobar el estado de la función HttpOnly

```
show aaa parameter
<!--NeedCopy-->
```

Limitaciones

- Cuando la función HttpOnly está habilitada, el botón de página de inicio del cliente Citrix Secure Access no funciona.
- El indicador HttpOnly no está establecido en ninguna autenticación clásica.

Personalizar el portal de usuarios de VPN

March 27, 2024

Las instalaciones de NetScaler Gateway que ofrecen el portal a los usuarios de VPN incluyen la opción de seleccionar un tema del portal para crear un aspecto personalizado para las páginas del portal. Puede seleccionar entre un conjunto de temas suministrado o puede usar un tema como plantilla para crear un portal personalizado o de marca. Con la utilidad de configuración, puede modificar un tema añadiendo nuevos logotipos, imágenes de fondo, etiquetas de cuadro de entrada personalizadas y varios otros atributos del diseño del portal basado en CSS. Los temas integrados del portal incluyen contenido para cinco idiomas: inglés, francés, español, alemán y japonés. Se atiende a diferentes usuarios en distintos idiomas, según las configuraciones regionales indicadas por sus exploradores web.

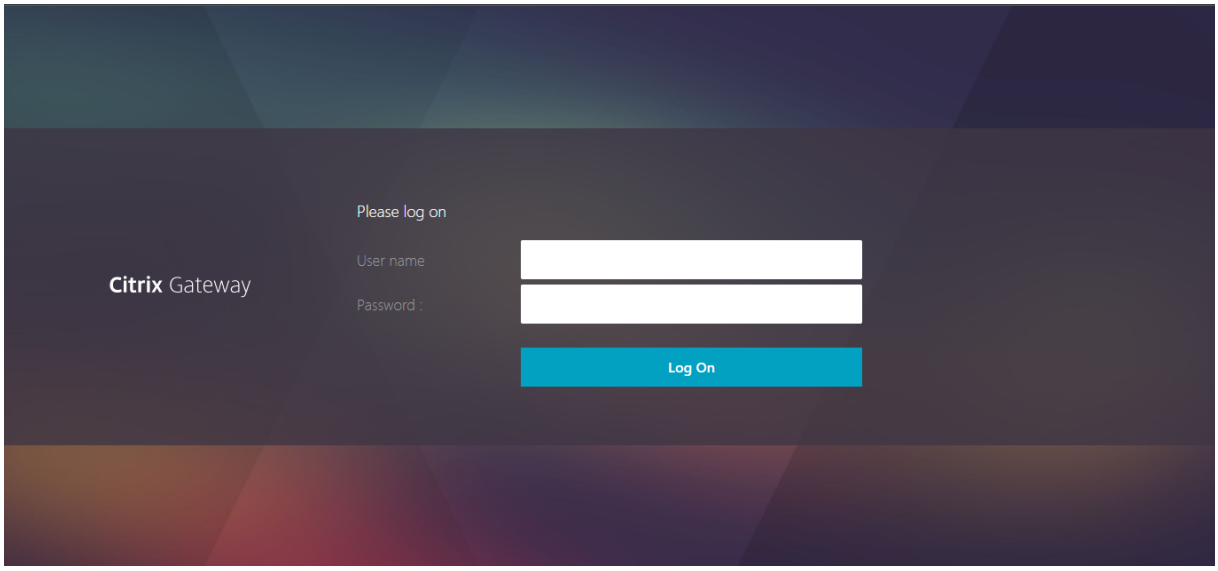
Puede crear un CLUF personalizado que se presente a los usuarios de VPN antes de que se les permita iniciar sesión. La función EULA admite versiones específicas de la configuración regional de un CLUF, que se presentan a los usuarios en función de las configuraciones regionales informadas de sus exploradores web.

Tanto los temas del portal como las configuraciones de EULA se pueden enlazar de forma independiente en el servidor virtual VPN y a nivel global de VPN.

> **Importante:**
>
> NetScaler no admite la personalización que requiera modificaciones en el código y no ofrece soporte para resolver problemas más allá de volver a un tema predeterminado.

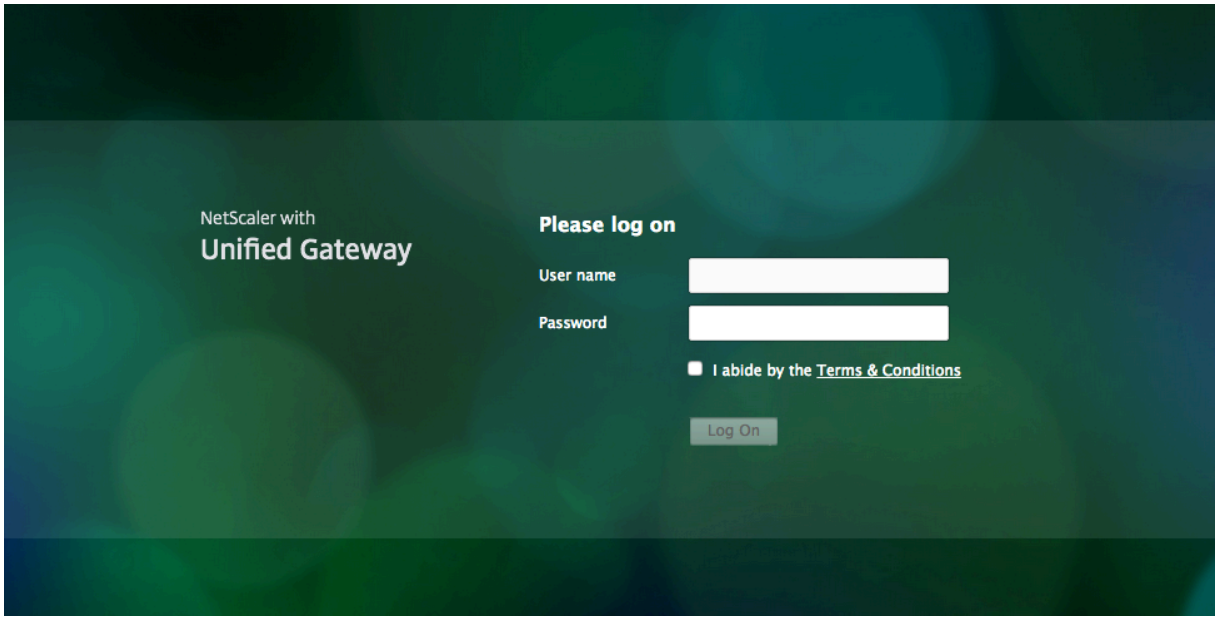
Aplicar un tema de portal

A partir de la versión 13.0 build 67.43, el portal VPN está configurado para usar el tema RfWebUI de forma predeterminada. Anteriormente, `Caxton theme` era el tema predeterminado. También puede aplicar los temas de Green Bubble y X1.

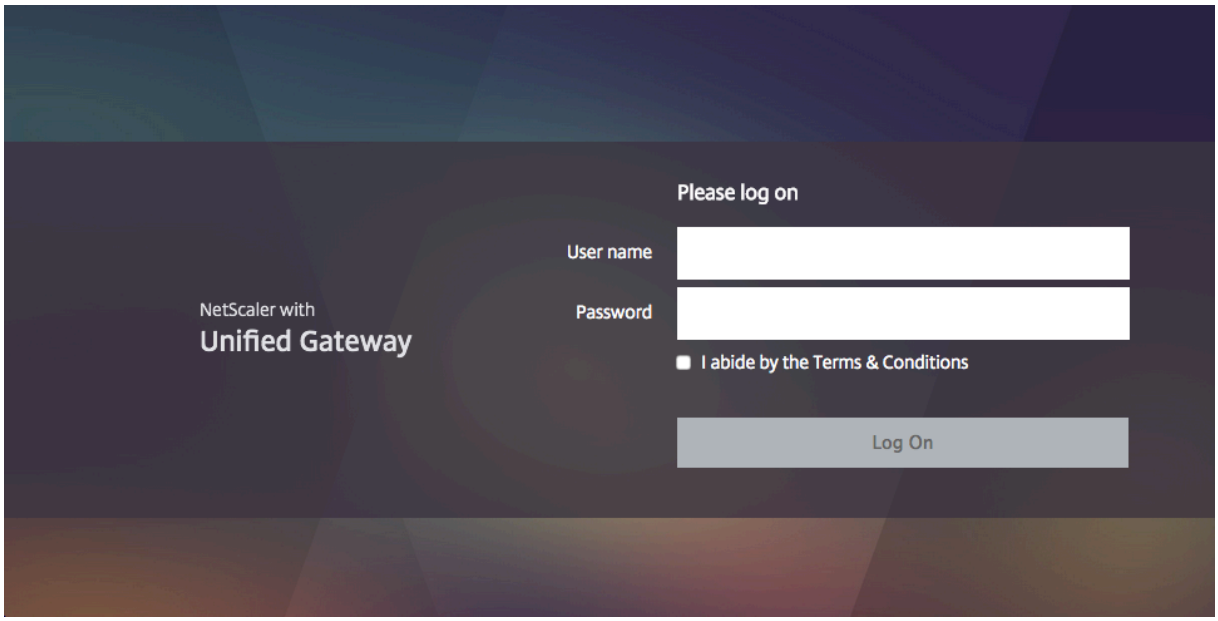


Tema Caxton

Tema de Green Bubble



Tema X1



Puede aplicar cualquiera de los temas suministrados directamente a un servidor virtual VPN o como enlace VPN global.

Enlazar un tema de portal a un servidor virtual VPN

Puede enlazar un tema de portal en un servidor virtual existente o al crear un nuevo servidor virtual.

Enlazar un tema de portal a un servidor virtual VPN mediante la CLI

En la línea de comandos, escriba;

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

Enlazar un tema de portal a un servidor virtual VPN mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Servidores virtuales.**
2. Seleccione un servidor virtual y, a continuación, haga clic en **Modificar**.
3. Si un tema del portal aún no se ha enlazado al servidor virtual, haga clic en **Tema del portal** en **Configuración avanzada** en el panel de detalles. De lo contrario, la opción **Tema del portal**ya está expandida en el panel de detalles.
4. En el panel de detalles, en **Temas del portal**, haga clic en **Sin tema del portal**para expandir la ventana de enlace Tema del portal.
5. `Click` **Haga clic para seleccionar**.
6. En la ventana **Temas del portal**, haga clic en un nombre de tema y, a continuación, haga clic en **Seleccionar**.
7. Haga clic en **Bind**.
8. Haga clic en **Listo**.

Si va a crear un servidor virtual VPN, puede seguir los pasos del procedimiento anterior comenzando por el paso 3 en el panel de **modificación del servidor virtual VPN** para enlazar un tema del portal.

Enlazar un tema de portal a VPN global

Enlazar un tema de portal a VPN global mediante la CLI

En la línea de comando, escriba;

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

Enlazar un tema de portal a VPN global mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **NetScaler Gateway.**
2. En el panel de detalles principal, haga clic en **NetScaler Gateway Policy Manager**.
3. Haga clic en el icono "**+**".
4. En la lista **Punto de enlace**, seleccione **Recursos**.
5. En la lista**Tipo de conexión**, seleccione**Tema del portal.**

6. Haga clic en **Continuar**.
7. En la pantalla **Punto de enlace**, haga clic en **Agregar enlace**.
8. Haga clic **en Haga clic para seleccionar**.
9. En la ventana **Temas del portal**, haga clic en un nombre de tema y, a continuación, haga clic en **Seleccionar**.
10. Haga clic en **Bind**.
11. Haga clic en **Cerrar**.
12. Haga clic en **Listo.**

> **Nota:**
>
> Tras realizar los cambios, utilice el comando «save ns config» en la línea de comandos o haga clic en el icono de guardar de la utilidad de configuración para asegurarse de que los cambios se guardan en el archivo de configuración de NetScaler.

Crear un tema de portal

Para crear un diseño de portal personalizado, utilice uno de los temas del portal suministrados como plantilla. El sistema hace una copia del tema de plantilla seleccionado con el nombre que especifique.

Usar un tema de portal de acciones como plantilla para un tema de portal personalizado

Para crear un tema del portal, puede utilizar la utilidad de configuración o la línea de comandos para crear la entidad del tema. Sin embargo, los controles de personalización detallados solo están disponibles en la utilidad de configuración.

Crear un tema de portal mediante la CLI

En la línea de comando, escriba;

```
add portaltheme <name> basetheme <name>
<!--NeedCopy-->
```

Crear un tema de portal mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Temas del portal**.
2. En el panel de detalles principal, haga clic en **Agregar**.

3. Escriba un nombre para el tema y seleccione una plantilla de la lista de plantillas y, a continuación, haga clic en **Aceptar**.
4. En este punto, se le presenta la primera vista de la ventana de modificación del tema del portal. Haga clic en **Aceptar** para salir.

Puede proceder a personalizar el nuevo tema del portal con la primera vista.

Una vez creado un nuevo tema, puede vincularlo a un servidor virtual VPN o a VPN global. Puede enlazar un nuevo tema inmediatamente después de crearlo o después de completar tus personalizaciones.

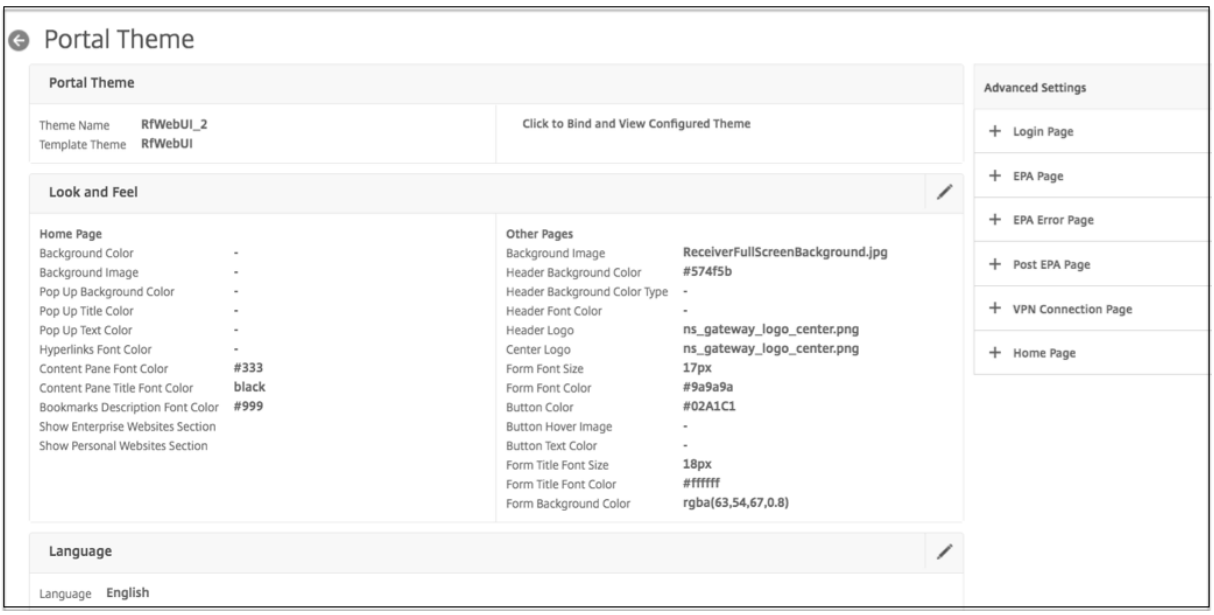
Personalización del tema del portal

Para personalizar un tema del portal, utilice la interfaz Tema del portal en la utilidad de configuración. Para obtener los mejores resultados, debe comprender los distintos elementos de esta interfaz antes de utilizarla.

Acerca de la interfaz del tema del portal

Para abrir la **interfaz del tema del portal** en la utilidad de configuración de NetScaler Gateway, en la ficha **Configuración**, vaya a **NetScaler Gateway** y haga clic en **Temas del portal**. Puede crear un tema como se describe en *Creación de un tema de portal* o seleccionar un tema existente en el panel de detalles principal y hacer clic en **Modificar**.

La página de personalización del tema del portal tiene cuatro paneles de componentes principales para modificar el diseño del **portal: el panel Tema** del portal, el panel Look & Feel, el panel **Configuración avanzada** y el panel **Idioma** .



El panel **Tema del portal** en la parte superior de la página informa qué tema se carga para modificar y en qué tema de plantilla se basa. La opción de visualización aquí le permite ver sus personalizaciones sin tener que acceder a la VPN con una conexión de usuario. El uso de la opción de visualización requiere vincular el tema a un servidor virtual VPN y el enlace permanece en vigor después de cerrar la ventana de visualización.

Con el panel **Aspecto y sensación** en el centro de la página, configura las propiedades generales de un tema, como encabezados, colores e imágenes de fondo, propiedades de fuente y logotipos. Cuando este panel está en modo de modificación, las leyendas de atributos están disponibles para obtener información sobre dónde se utilizan los atributos Aspecto y sensación en las páginas del portal.

El panel **Configuración avanzada** contiene los controles de contenido en pantalla de las páginas del portal individuales. Para cargar el contenido de una página para modificarlo, haga clic en una de las páginas de la lista. Los controles de página se abren debajo de los demás paneles centrales. Una página permanece contraída en el panel **Configuración avanzada** en todas las ediciones del tema del portal siempre y cuando la página no se haya modificado.

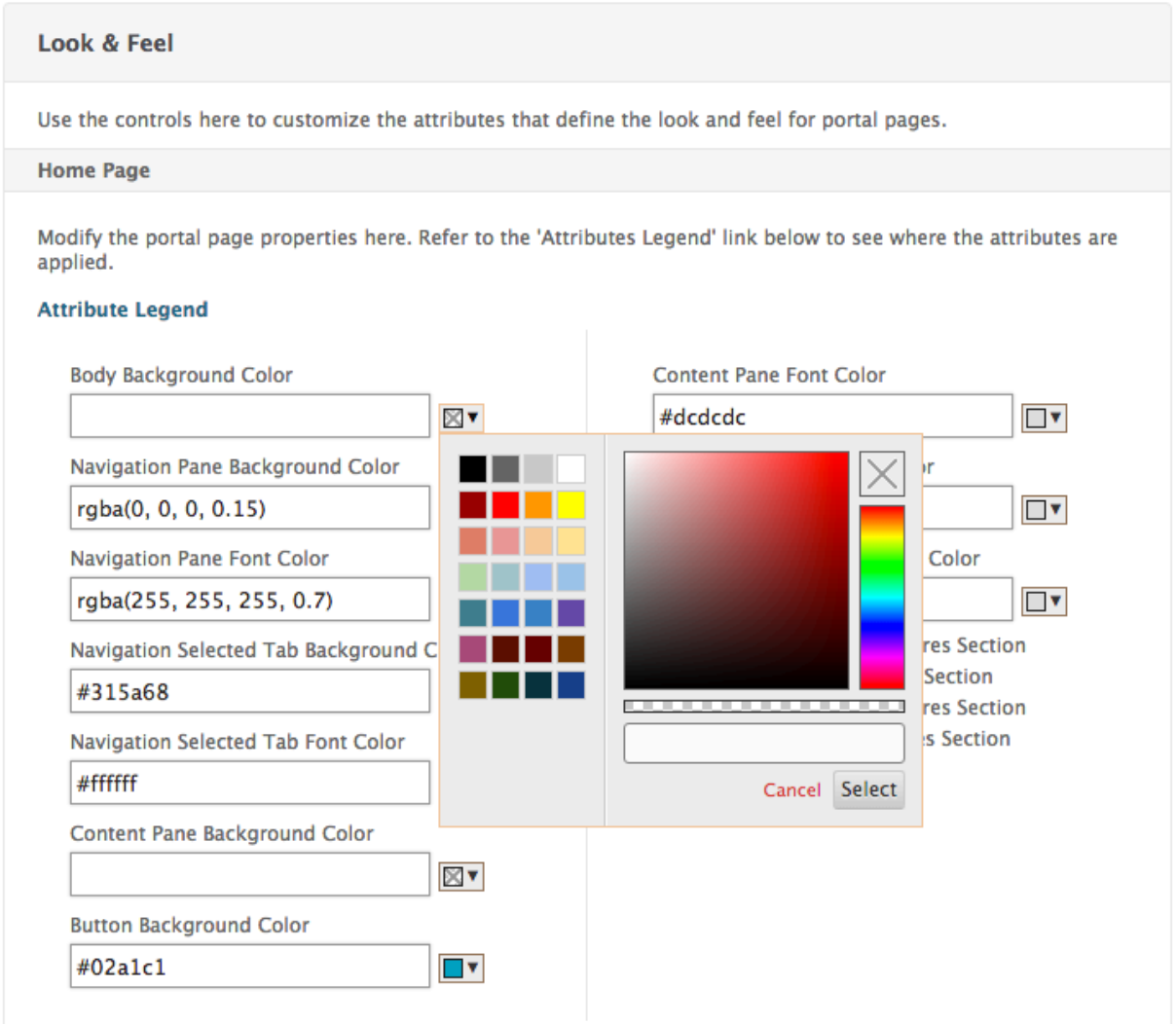
En el panel **Idioma**, puede seleccionar cuál de los idiomas se carga cuando se selecciona una página para modificarla en el panel **Configuración avanzada**. Las páginas en inglés se cargan de forma predeterminada.

Tipos de atributos de página personalizables

Al personalizar un tema del portal, puede modificar una serie de atributos en la interfaz del tema del portal. Junto con el texto y los idiomas compatibles que se pueden modificar, los elementos gráficos del diseño del portal se pueden adaptar a sus necesidades. Cada tipo de elemento de página tiene parámetros o recomendaciones que se deben tener en cuenta antes de modificarlos.

Colores

El diseño del portal especifica los colores de los atributos como fondos de página, resaltados, texto para títulos y contenido principal, controles de botones y respuestas al pasar el ratón. Para personalizar un atributo de color, puede introducir un valor de color directamente para un artículo seleccionado o utilizar el selector de color suministrado para generar un valor de color. La interfaz admite la introducción de valores de color HTML válidos en formato RGBA, formato triplete hexadecimal HTML y nombres de colores X11. Se puede acceder al selector de color para cualquier atributo de color aplicable haciendo clic en el cuadro de color junto al campo de entrada del atributo.



Fuentes

Junto con los colores de las fuentes, puede modificar el tamaño de fuente de algunos atributos de página. Para cada uno de estos atributos, un menú ofrece los tamaños disponibles para cada atributo, según lo determine el diseño del portal.

Imágenes

En el caso de las imágenes, una descripción emergente disponible para cada control proporciona recomendaciones de tamaño y otros requisitos. Las descripciones varían según la ubicación de un atributo en la página y su función. Puede utilizar formatos de archivo de imagen PNG o JPEG. Para seleccionar una imagen para cargarla, selecciona la casilla situada debajo del nombre de archivo del elemento y, a continuación, navega hasta la ubicación de la imagen en la unidad de disco de tu ordenador local.

Etiquetas

En la sección **Configuración avanzada**, puede seleccionar el texto de una página de portal específica

para modificar. Si modifica el texto en inglés predeterminado de una página, el texto de otros idiomas no se vuelve a traducir. El contenido de la página de idioma alternativo se proporciona para su comodidad, pero requiere actualizaciones manuales para cualquier personalización. Para modificar otra versión de idioma de una página, contrae primero la ventana, si está abierta, haciendo clic en el icono **X** de la página del portal abierta. A continuación, seleccione el idioma en el panel **Idioma** y haga clic en **Aceptar**. Todas las páginas del portal que se abren desde el panel **Configuración avanzada** están en ese idioma hasta que seleccione una diferente.

> **Importante**
>
> En implementaciones de alta disponibilidad o agrupadas, los temas del portal se distribuyen a través de la configuración compartida solo cuando la configuración del tema del portal se realiza en las entidades NetScaler principal o coordinador de configuración, respectivamente.

Personalizaciones del portal más antiguas

Para las instalaciones con un diseño de portal personalizado modificado manualmente y creado en las versiones de NetScaler Gateway o Access Gateway anteriores a la 11.0, NetScaler recomienda encarecidamente empezar con un nuevo tema de portal en la interfaz de personalización. Si no puede hacerlo, puede aplicar una personalización manualmente, pero no se proporciona soporte directo para ello.

Al utilizar un portal personalizado manualmente, debe establecer el portal personalizado como una configuración de portal global. Sin embargo, hacerlo significa que una configuración de portal global aplicada *no se puede* anular con los enlaces de tema del portal a nivel de servidor virtual VPN. Intentar crear un enlace de servidor virtual VPN en este caso con la utilidad de configuración o la línea de comandos devuelve un error.

Además, en el caso de configuraciones de clúster y alta disponibilidad, las personalizaciones manuales deben realizarse en todos los nodos de la implementación, ya que los archivos subyacentes del sistema de archivos NetScaler no se distribuyen en la configuración compartida automáticamente.

Crear manualmente una configuración de portal personalizada

Para aplicar manualmente una configuración de portal personalizada anterior después de actualizar a NetScaler Gateway 11.0, debe modificar una copia de una página de portal existente, colocar los archivos de portal personalizados en el sistema de archivos NetScaler y seleccionar **CUSTOM** como parámetro **UITHEME**.

Puede utilizar WinSCP o cualquier otro programa de copia segura para transferir archivos al sistema de archivos NetScaler.

1. Inicie sesión en la línea de comandos de NetScaler Gateway.

2. En el símbolo del sistema, escriba**shell**
3. En el símbolo del sistema, escriba **mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*.**
4. En el símbolo del sistema, escriba **cd /var/netscaler/logon/themes/**

    - Si quieres personalizar el tema de la burbuja verde, introduzca **cp -r** `Greenbubble` **Custom** para hacer una copia del tema de Green Bubble.
    - Si quieres personalizar el tema por defecto (`Caxton`), escribe **cp -r Default Custom.**
    - Para personalizar el tema X1, escriba**cp -r X1 Custom.**

5. Realice los cambios necesarios en los archivos copiados en**/var/NetScaler/logon/themes/custom** para personalizar el tema manualmente.

    - Realice las ediciones necesarias en **css/base.css**.
    - Copie las imágenes personalizadas en el directorio **/var/ns_gui_custom/ns_gui/vpn/media**.
    - Realice cambios en las etiquetas de los archivos presentes en el directorio **resources/**. Estos archivos corresponden a las configuraciones regionales compatibles con el portal.
    - Si también se necesitan cambios en las páginas HTML o en los archivos javascript, puede hacer lo relevante para los archivos en **/var/ns_gui_custom/ns_gui/**.

6. Una vez que se hayan completado todos los cambios de personalización, escriba: **tar —cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/***

> **Importante**
>
> Al copiar un directorio de temas en los pasos anteriores, el nombre de carpeta copiada debe escribirse exactamente como "Personalizado", ya que los nombres de directorio distinguen entre mayúsculas y minúsculas dentro de la interfaz de shell de NetScaler. Si el nombre del directorio no se introduce con precisión, la carpeta no se reconoce cuando la configuración **UITHEME** está configurada en **CUSTOM**.

Seleccione el tema personalizado como parámetro global de VPN

Una vez finalizada la configuración del portal personalizada manualmente y copiada en el sistema de archivos NetScaler, debe aplicarse a la configuración de NetScaler Gateway. Esto se hace estableciendo el parámetro UITHEME en CUSTOM y se puede completar con la línea de comandos o la utilidad de configuración.

Para utilizar la línea de comandos, escriba el siguiente comando para establecer el parámetro **UITHEME**.

```
set vpn parameter UITHEME CUSTOM
<!--NeedCopy-->
```


Para establecer el parámetro UITHEME mediante la utilidad de configuración, utilice el procedimiento siguiente.

1. En la ficha **Configuración**, vaya a **NetScaler Gateway > Configuración global**.
2. Haga clic en **Cambiar configuración global**.
3. Haga clic en la ficha **Experiencia del cliente**.
4. Vaya hasta la parte inferior de la pantalla y seleccione **PERSONALIZAR** en el menú de lista de **temas de la interfaz** de usuario.
5. Haga clic en **Aceptar**.

El portal personalizado manualmente es ahora el diseño del portal presentado a los usuarios de VPN.

Crear un EULA

El sistema de portal VPN ofrece la opción de aplicar un CLUF a la configuración de un portal. Una vez que un CLUF está vinculado a la configuración de NetScaler Gateway, ya sea en el ámbito global de VPN o en un servidor virtual VPN relevante, los usuarios de VPN deben aceptar el CLUF como términos y condiciones antes de que se les permita autenticarse en la VPN.

Al igual que con los temas del portal, los usuarios reciben un EULA específico para el idioma en función de la configuración regional indicada por su navegador web. En el caso de una configuración regional que no coincida con ninguno de los idiomas admitidos, el idioma predeterminado que se sirve es el inglés. Para cada EULA, puede introducir un mensaje personalizado en cada uno de los idiomas admitidos. El contenido pretraducido no se proporciona para las configuraciones del CLUF como lo es para los temas del portal.Si la configuración regional notificada de un usuario coincide con un idioma en el que no se ha introducido ningún contenido del CLUF, se le devuelve una página en blanco cuando hace clic en el enlace "Términos y condiciones"de la página de inicio de sesión de VPN.

Para crear un CLUF, puede utilizar cualquiera de los controles de la utilidad de configuración de la ficha **Configurar NetScaler Gateway**** > Configuración global > CLUF**o**NetScaler Gateway > Recursos > CLUF**. Los controles del panel**Configuración global**se utilizan para administrar los enlaces de EULA globales de VPN, mientras que el control del nodo**Recursos > EULA**se utiliza para operaciones generales en configuraciones de EULA. Puede administrar los enlaces de EULA del servidor virtual VPN editando un servidor virtual VPN en**NetScaler Gateway > Servidores virtuales**. Algunos comandos también están disponibles con la línea de comandos para administrar entidades de CLUF. Sin embargo, los controles completos de administración del CLUF solo están disponibles en la utilidad de configuración.

Crear una entidad de EULA mediante la CLI

En la línea de comandos, escriba;


```
add vpn eula <name>
<!--NeedCopy-->
```

Crear una entidad EULA mediante la GUI

1. Vaya a **NetScaler Gateway > Recursos > EULA**.
2. Haga clic en **Agregar** para crear una entidad.
3. Introduzca un nombre para la entidad.
4. Para cada uno de los idiomas, pega el contenido en las fichas correspondientes.
5. Haga clic en **Crear**.

A partir de la versión 14.1, compilación 17.38, se vuelven a habilitar las siguientes etiquetas HTML en el texto del EULA. Estas etiquetas se deben usar sin los atributos HTML.

```
- <html></html>
- <b></b>
- <p></p>
- <i></i>
- <ol></ol>
- <ul></ul>
- <li></li>
- <br></br><br/>
<!--NeedCopy-->
```

Una vez creada una entidad EULA, se puede enlazar globalmente a la configuración de VPN o a un servidor virtual VPN.

Vincular un CLUF a una VPN global mediante la CLI

En la línea de comando, escriba;

```
bind vpn global eula <name>
<!--NeedCopy-->
```

Vincular un CLUF a una VPN global mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **NetScaler Gateway > Configuración global**.
2. En el panel de detalles principal, haga clic en **Configurar un contrato de licencia de usuario final**.
3. Haga clic en **Add Binding**.
4. Haga clic **en Haga clic para seleccionar**.
5. Seleccione una entidad EULA y, a continuación, haga clic en **Seleccionar**.

6. Haga clic en **Bind**.
7. Haga clic en **Cerrar**.

Vincular un CLUF a un servidor virtual VPN mediante la CLI

En la línea de comando, escriba;

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```

Enlazar un CLUF a un servidor virtual VPN mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **NetScaler Gateway > Servidores virtuales.**
2. En el panel de detalles principal, seleccione un servidor virtual VPN y haga clic en **Modificar**.
3. En el panel **Configuración avanzada** de la parte derecha de la página, haga clic en **CLUF**.
4. En el panel CLUF recién agregado, haga clic en **Sin EULA**.
5. `Click` **Haga clic para seleccionar**.
6. Seleccione una entidad EULA y haga clic en **Seleccionar**.
7. Haga clic en **Bind**.
8. Haga clic en **Listo**.

Solicitar a los usuarios que actualicen exploradores antiguos o no compatibles mediante la creación de una página personalizada

January 26, 2024

Si un cliente se conecta a una dirección VIP de NetScaler mediante un cifrado no seguro, como SSLv3, se le puede redirigir a una página personalizada en la que se le pida que actualice a la versión más reciente de Internet Explorer, Firefox, Chrome o Safari.

Nota: Según RFC6176 del Grupo de trabajo de ingeniería de Internet (ITEF), los servidores TLS no deben ser compatibles con SSLv2. Por lo tanto, el dispositivo NetScaler no admite SSLv2 de la versión 12.1 y posteriores.

Cómo crear una página personalizada para pedir a los usuarios que actualicen exploradores antiguos no compatibles basados en SSL

- Cree una directiva de respuesta de NetScaler con la regla `client.ssl.version.eq()`. La versión devuelve la versión del protocolo SSL.

  - Devuelve 0 si la transacción no está basada en SSL.
  - Devuelve 0x002 si la transacción es SSLv2.
  - Devuelve 0x300 si la transacción es SSLv3.
  - Devuelve 0x301 si la transacción es TLSv1.

- Debe habilitar SSLv3 (u otra versión anterior) para activar la directiva de respuesta.

  Por ejemplo, si SSLv3 está inhabilitado en el dispositivo NetScaler y un cliente con un explorador antiguo que utiliza SSLv3 intenta conectarse, se deniega el acceso.

- Si la implementación requiere SSLv3 o una versión anterior durante un período específico (uno o dos meses), configure lo siguiente:

  - Habilite el protocolo SSLv3.
  - Actualice la página personalizada para incluir información de que, transcurrido el período especificado, el explorador no puede conectarse al dispositivo.

Configurar el acceso VPN sin cliente con NetScaler Gateway

March 27, 2024

El acceso sin cliente permite a los usuarios el acceso que necesitan sin necesidad de instalar software de usuario, como el cliente Citrix Secure Access o Receiver. Los usuarios pueden utilizar su explorador web para conectarse a aplicaciones web, como Outlook Web Access.

Siga los pasos siguientes para configurar el acceso sin cliente:

- Habilitar el acceso sin cliente de forma global o mediante una directiva de sesión vinculada a un usuario, grupo o servidor virtual.
- Selección del método de codificación de direcciones web.

Para habilitar el acceso sin cliente solo para un servidor virtual específico, inhabilite el acceso sin cliente globalmente y, a continuación, cree una directiva de sesión para habilitarlo.

Si utiliza el asistente de NetScaler Gateway para configurar el dispositivo, tiene la opción de configurar el acceso sin cliente en el asistente. La configuración del asistente se aplica de forma global. En el asistente de NetScaler Gateway, puede configurar los siguientes métodos de conexión de clientes:

- Cliente Citrix Secure Access. Los usuarios pueden iniciar sesión únicamente mediante el cliente Citrix Secure Access.
- Utilice el cliente Citrix Secure Access y permita el escenario de acceso alternativo. Los usuarios inician sesión en NetScaler Gateway con el cliente Citrix Secure Access. Si el dispositivo de usuario no supera la exploración de análisis de dispositivos de punto final, los usuarios pueden

iniciar sesión mediante el acceso sin cliente. Cuando esto ocurre, los usuarios tienen acceso limitado a los recursos de red.
- Permitir que los usuarios inicien sesión mediante un explorador web y acceso sin cliente. Los usuarios solo pueden iniciar sesión mediante el uso de acceso sin cliente y recibir acceso limitado a los recursos de red.

Cómo funcionan las directivas de acceso a VPN sin cliente

El acceso sin cliente a las aplicaciones web se configura mediante la creación de directivas. Puede configurar la configuración de una directiva de acceso sin cliente en la utilidad de configuración. Una directiva de acceso sin cliente se compone de una regla y un perfil. Puede utilizar las directivas de acceso sin cliente preconfiguradas que vienen con NetScaler Gateway. También puede crear sus propias directivas de acceso sin cliente personalizadas.

NetScaler Gateway proporciona directivas preconfiguradas para lo siguiente:

- Outlook Web Access y Outlook Web App
- SharePoint 2007
- Todas las demás aplicaciones web

> **Nota:**
>
> OWA 2016 y SharePoint 2016 solo son compatibles con el acceso avanzado sin cliente.

Tenga en cuenta las siguientes funciones de las directivas de acceso sin cliente preconfiguradas:

- Se configuran automáticamente y no se pueden cambiar.
- Cada directiva está vinculada a nivel global.
- Cada directiva no se aplica a menos que habilite el acceso sin cliente de forma global o mediante la creación de una directiva de sesión.
- No puede quitar ni modificar los enlaces globales, aunque no habilite el acceso sin cliente.

La compatibilidad con otras aplicaciones web depende de las directivas de reescritura configuradas en NetScaler Gateway. Citrix recomienda probar todas las directivas personalizadas que cree para asegurarse de que todos los componentes de la aplicación se reescriban correctamente.

Si permite conexiones desde Receiver para Android, Receiver para iOS o Citrix Secure Hub, debe habilitar el acceso sin cliente. Para Citrix Secure Hub que se ejecuta en un dispositivo iOS, también debe habilitar Secure Browse en el perfil de sesión. Secure Browse y el acceso sin cliente funcionan conjuntamente para permitir conexiones desde dispositivos iOS. No tiene que habilitar Secure Browse si los usuarios no se conectan con dispositivos iOS.

El asistente de configuración rápida configura las directivas y la configuración de acceso sin cliente correctas para los dispositivos móviles. Citrix recomienda ejecutar el Asistente de configuración ráp-

ida para configurar las directivas correctas para las conexiones a StoreFront y Citrix Endpoint Management.

Puede enlazar directivas de acceso sin cliente personalizadas de forma global o a un servidor virtual. Si quiere vincular directivas de acceso sin cliente a un servidor virtual, debe crear una directiva personalizada y, a continuación, vincularla. Para aplicar directivas diferentes para el acceso sin cliente, ya sea de forma global o para un servidor virtual, cambie el número de prioridad de la directiva personalizada para que tenga un número inferior al de las directivas preconfiguradas, dando así mayor prioridad a la directiva personalizada. Si no hay ninguna otra directiva de acceso sin cliente vinculada al servidor virtual, las directivas globales preconfiguradas tienen prioridad.

> **Nota:**
>
> No se pueden cambiar los números de prioridad de las directivas de acceso sin cliente preconfiguradas.

Habilitar el acceso VPN sin cliente

Al habilitar el acceso sin cliente a nivel global, todos los usuarios reciben la configuración del acceso sin cliente. Puede utilizar el asistente de NetScaler Gateway, una directiva global o una directiva de sesión para habilitar el acceso sin cliente.

En una configuración global o en un perfil de sesión, el acceso sin cliente tiene la siguiente configuración:

- **Enciendo**. Permite el acceso sin cliente. Si inhabilita las opciones del cliente y no configura ni inhabilita StoreFront, los usuarios inician sesión mediante el acceso sin cliente.
- **Desactivado**. El acceso sin cliente no está habilitado de forma predeterminada. El acceso sin cliente se habilita después de que los usuarios inicien sesión con el cliente Citrix Secure Access. Si deshabilita las opciones de cliente y no configura ni deshabilita StoreFront, los usuarios iniciarán sesión con el cliente Citrix Secure Access. Si el análisis de dispositivos de punto final falla cuando los usuarios inician sesión, los usuarios reciben la página de opciones con acceso sin cliente disponible.
- **Inhabilitado**. El acceso sin cliente está inhabilitado. Al seleccionar **Inhabilitado**, los usuarios no pueden iniciar sesión mediante el acceso sin cliente y el icono de acceso sin cliente no aparece en la página de opciones.

Si no habilita el acceso sin cliente mediante el asistente de NetScaler Gateway, puede habilitarlo globalmente o en una directiva de sesión mediante la utilidad de configuración.

Para habilitar el acceso sin cliente de forma global

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.**
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, junto a **Acceso sin cliente**, seleccione ACTIVADO y **, a continuación,** haga clic en **Aceptar**.

Para habilitar el acceso sin cliente mediante una directiva de sesión

Si quiere que solo un grupo selecto de usuarios, grupos o servidores virtuales utilice el acceso sin cliente, desactive o borre el acceso sin cliente de forma global. A continuación, mediante una directiva de sesión, habilite el acceso sin cliente y vincúlelo a usuarios, grupos o servidores virtuales.

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la pestaña **Experiencia del cliente** , junto a Acceso sin cliente, haga clic en **Anular global** , seleccione Activado y**,** a continuación , haga clic en **Crear**.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione General, seleccione Valor verdadero, haga clic en Agregar expresión, en **Crear** y, a continuación, en **Cerrar**.
8. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Después de crear la directiva de sesión que permite el acceso sin cliente, la vincula a un usuario, grupo o servidor virtual.

Codificar la dirección web

Al habilitar el acceso sin cliente, puede optar por codificar las direcciones de las aplicaciones web internas o dejar la dirección como texto sin cifrar. Los ajustes son los siguientes:

- Oscuro. Utiliza mecanismos de codificación estándar para ocultar la parte del dominio y el protocolo del recurso.
- Claro. La dirección web no está codificada y es visible para los usuarios.
- Cifrar. El dominio y el protocolo se cifran mediante una clave de sesión. Cuando la dirección web está cifrada, la URL es diferente para cada sesión de usuario del mismo recurso web. Si los usuarios marcan la dirección web codificada como marcador, la guardan en el explorador web

y luego cierras la sesión, cuando los usuarios inician sesión e intentan conectarse de nuevo a la dirección web mediante el marcador, no podrán conectarse a la dirección web.
Nota: Si los usuarios guardan el marcador cifrado en la interfaz de acceso durante su sesión, el marcador funciona cada vez que el usuario inicia sesión.

Puede configurar esta configuración de forma global o como parte de una directiva de sesión. Si configura la codificación como parte de la directiva de sesión, puede vincularla a los usuarios, grupos o un servidor virtual.

Configurar la codificación de direcciones web de forma global

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, junto a Codificación URL de acceso sin cliente, seleccione el nivel de codificación y, a continuación, haga clic en Aceptar.

Configurar la codificación de direcciones web mediante la creación de una directiva de sesión

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, junto a Codificación URL de acceso sin cliente, haga clic en Anular global, seleccione el nivel de codificación y, a continuación, haga clic en Aceptar.
7. En el cuadro de diálogo Crear política de sesión , junto a Expresiones con nombre, seleccione General , seleccione Valor verdadero , haga clic en Agregar expresión , en Crear y, a continuación, en Cerrar .

Crear directivas de acceso sin cliente

Si quiere utilizar la misma configuración que para las directivas de acceso sin cliente predeterminadas pero quiere enlazar la directiva a un servidor virtual, puede copiar las directivas predeterminadas y proporcionar un nuevo nombre para la directiva. Puede utilizar la utilidad de configuración para copiar las directivas predeterminadas.

Después de enlazar la nueva directiva al servidor virtual, puede establecer la prioridad de la directiva para que se ejecute primero cuando un usuario inicie sesión.

Crear una directiva de acceso sin cliente mediante la configuración predeterminada

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Acceso sin cliente.
2. En el panel de detalles, en la ficha Directivas, haga clic en una directiva predeterminada y, a continuación, haga clic en Agregar.
3. En Nombre, escriba un nombre nuevo para la directiva, haga clic en Crear y, a continuación, haga clic en Cerrar.

Enlazar una directiva de acceso sin cliente a un servidor virtual

Después de crear la directiva, enlaza la directiva al servidor virtual.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, seleccione un servidor virtual y, a continuación, haga clic en Abrir .
3. En el cuadro de diálogo configurar el servidor virtual de NetScaler Gateway, haga clic en la ficha Directivas y, a continuación, haga clic en Sin cliente.
4. Haga clic en Insertar directiva, seleccione una directiva de la lista y, a continuación, haga clic en Aceptar.

Crear y evaluar expresiones de directiva de acceso sin cliente

Al crear una directiva de acceso sin cliente, puede crear su propia expresión para la directiva. Cuando haya terminado de crear la expresión, podrá evaluar la exactitud de la expresión.

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Acceso sin cliente.
2. En el panel de detalles, en la ficha Directivas, haga clic en una directiva predeterminada y, a continuación, haga clic en Agregar.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. Configure los ajustes de reescritura y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear directiva de acceso sin cliente, en Expresión, haga clic en Agregar.
8. En el cuadro de diálogo Agregar expresión, cree la expresión y, a continuación, haga clic en Aceptar.

9. En el cuadro de diálogo Crear directiva de acceso sin cliente, haga clic en Evaluar y, si la expresión es correcta, haga clic en Crear.

Acceso VPN avanzado sin cliente con NetScaler Gateway

March 27, 2024

La VPN sin cliente ve una forma de proporcionar acceso remoto a los recursos de la intranet de la empresa a través de NetScaler Gateway sin una aplicación cliente VPN en el equipo cliente. La VPN sin cliente proporciona acceso remoto a aplicaciones web empresariales, portales y otros recursos mediante un explorador web en el extremo del cliente.
La solución VPN avanzada sin cliente elimina las siguientes limitaciones relacionadas con la VPN sin cliente:

- Las URL relativas no se pueden identificar a veces.
- Las URL relativas generadas dinámicamente no se pueden identificar.

La VPN avanzada sin cliente identifica la URL absoluta y los nombres de host y los reescribe de una manera nueva y única en lugar de intentar reescribir las URL relativas presentes en las páginas web o respuestas HTTP. SharePoint ya no necesita usar la carpeta predeterminada para reescribir direcciones URL y se admite un acceso personalizado a SharePoint.

Requisitos previos

Los siguientes son los requisitos previos para configurar la VPN avanzada sin cliente.

- **Certificado de servidor Wildcard** : la VPN avanzada sin cliente reescribe las URL de una manera única. Esta singularidad se mantiene para cada URL por usuario. Por ejemplo, si la aplicación web está alojada en `https://webapp.customer.com`, y el servidor virtual VPN está alojado en `https://vpn.customer.com`, la VPN avanzada sin cliente la reescribe como `https://cvpneqwerty.vpn.customer.com`. Esto significa que cada URL se reescribe como subdominio del servidor virtual VPN. En esta nueva URL, `cvpneqwerty` se puede descifrar de vuelta a `https://webapp.customer.com`. La cadena `cvpneqwerty` es dinámica y, por lo tanto, para SSL, debe vincular el servidor virtual VPN con un certificado comodín.

  Si el servidor está alojado en `https://vpn.customer.com`, el certificado del servidor debe tener entradas para (vpn.customer.com y .vpn.customer.com) como parte de los certificados CN o SAN (donde CN = nombre común, SAN= nombre alternativo del sujeto). El proceso de vinculación de este certificado sigue siendo el mismo en NetScaler Gateway.

Nota: Los certificados comodín solo admiten un nivel (es decir, ..cliente.com no está permitido). Si ya utiliza un certificado comodín (para *.customer.com) y alojamiento `https://vpn.customer.com`, esto no funciona para la VPN avanzada sin cliente. Debe obtener un nuevo certificado con `*.vpn.customer.com`.

- **Entrada DNS comodín**: Los clientes (exploradores web) deben resolver el FQDN de la aplicación VPN avanzada sin cliente. Al configurar el servidor NetScaler Gateway, debe haber configurado una entrada DNS para resolver vpn.customer.com. Esto permite que el explorador resuelva vpn.customer.com en la dirección IP de su servidor virtual VPN. Para resolver direcciones URL como `https://cvpnqwerty.vpn.customer.com` en la misma IP (dirección IP del servidor virtual VPN), debe agregar un nuevo registro para el dominio de `vpn.customer.com` . Busque la configuración del dominio en su servidor DNS y agregue un nuevo registro de host para "*"con la misma dirección IP que antes. Después de agregar el registro de host, debe ver las respuestas ping correctas para `https://cpvnanything.vpn.customer.com`.

Configurar el acceso VPN avanzado sin cliente

Para configurar el acceso VPN avanzado sin cliente mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba:

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

Si una acción de sesión está vinculada al servidor virtual, debe habilitar también la opción Modo VPN avanzado sin cliente para esa acción de sesión.

Ejemplo:

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```

Para configurar el acceso VPN avanzado sin cliente mediante la GUI de NetScaler:

1. En la GUI de NetScaler, vaya a **Configuración > NetScaler > Configuración global**.
2. En la **página Configuración global**, haga clic en **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. En la ficha **Experiencia del cliente**, en la lista **Acceso sin cliente**, haga clic **en On**.
4. En la ficha **Experiencia del cliente**, en la lista **Modo VPN sin cliente avanzado**, haga clic en **Habilitado**.
   Si selecciona **STRICT** en la lista **Modo VPN sin cliente avanzado**, el dispositivo NetScaler solo responde a las URL de StoreFront en la forma clásica de VPN sin cliente y bloquea todas las

demás solicitudes VPN clásicas sin cliente. Esta opción proporciona una configuración más segura en el dispositivo para entregar recursos web internos.

> **Nota:**
>
> - Si una acción de sesión está enlazada al servidor virtual, debe habilitar la opción **Modo VPN sin cliente avanzado** para esa acción de sesión también desde la ficha **Experiencia del cliente** en la página **Configurar perfil de sesión de NetScaler Gateway**.
> - Puede seleccionar la opción **Supedición global** para anular la configuración global.
> - También puede configurar la función VPN avanzada sin cliente a nivel de sesión.

Advertencias

La VPN avanzada sin cliente tiene como objetivo proporcionar acceso a aplicaciones web empresariales. Estas aplicaciones solo tienen un FQDN para cada tipo de recurso que necesitan (JavaScript, css, imágenes, etc.). Dado que codificamos el FQDN completo de las aplicaciones internas en un solo octeto (VPN sin cliente), perdemos la relación de subdominio. Como resultado, cada vez que se configura una aplicación web empresarial con CORS, a veces se observan problemas al acceder a ella a través de la VPN avanzada sin cliente.

Configurar el acceso al dominio para los usuarios

March 27, 2024

Si los usuarios se conectan mediante el acceso sin cliente, puede restringir los recursos de red, los dominios y los sitios web a los que se permite el acceso de los usuarios. Puede utilizar el asistente de NetScaler Gateway o la configuración global para crear listas para incluir o excluir el acceso a los dominios.

Puede permitir el acceso a todos los recursos de red, dominios y sitios web y, a continuación, crear una lista de exclusión. La lista de exclusión cita un conjunto específico de recursos al que los usuarios no pueden acceder. Los usuarios no pueden acceder a los dominios incluidos en la lista de exclusión.

También puede denegar el acceso a todos los recursos de red, dominios y sitios web y, a continuación, crear una lista de inclusión específica. En la lista de inclusión se citan los recursos a los que pueden acceder los usuarios. Los usuarios no pueden acceder a ningún dominio que no aparezca en la lista.

Nota: Si configura directivas de acceso sin cliente para Citrix Endpoint Management o StoreFront y los usuarios se conectan con Receiver para Web, debe permitir los dominios a los que puede acceder Receiver para Web. Esto es necesario para que NetScaler Gateway pueda reescribir el tráfico de red de StoreFront y Endpoint Management.

Para configurar el acceso al dominio mediante el asistente de NetScaler Gateway

1. En la utilidad de configuración, haga clic en la pestaña Configuración y, a continuación, en el panel de navegación, haga clic en NetScaler Gateway .
2. En el panel de detalles, en Introducción, haga clic en el asistente de NetScaler Gateway .
3. Haga clic en Siguiente y, a continuación, siga las instrucciones del asistente hasta llegar a la página Configurar acceso sin cliente.
4. Haga clic en Configurar dominios para acceso sin cliente y realice una de las siguientes acciones:
    - Para crear una lista de dominios excluidos, haga clic en Excluir dominios.
    - Para crear una lista de dominios incluidos, haga clic en Permitir dominios.
5. En Nombres de dominio, escriba el nombre de dominio y, a continuación, haga clic en Agregar.
6. Repita el paso 5 para cada dominio que quiera agregar a la lista y, a continuación, haga clic en Aceptar cuando haya terminado.
7. Siga configurando el dispositivo mediante el asistente de NetScaler Gateway.

Para configurar la configuración del dominio mediante la utilidad de configuración

También puede crear o modificar la lista de dominios mediante la configuración global de la utilidad de configuración.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Acceso sin cliente, haga clic en Configurar dominios para acceso sin cliente.
3. Lleve a cabo una de las siguientes acciones:
    - Para crear una lista de dominios excluidos, haga clic en Excluir dominios.
    - Para crear una lista de dominios incluidos, haga clic en Permitir dominios.
4. En Nombres de dominio, escriba el nombre de dominio y, a continuación, haga clic en Agregar.
5. Repita el paso 4 para cada dominio que quiera agregar a la lista y, a continuación, haga clic en Aceptar cuando haya terminado.

Acceso VPN sin cliente para SharePoint 2003, SharePoint 2007 y SharePoint 2013

March 27, 2024

NetScaler Gateway puede reescribir el contenido de uno o más sitios de SharePoint 2003, SharePoint 2007 o SharePoint 2013 para que el contenido esté disponible para los usuarios sin necesidad del cliente Citrix Secure Access. Para que el proceso de reescritura se complete correctamente, debe configurar NetScaler Gateway con el nombre de host de cada servidor SharePoint de la red.

Puede utilizar el asistente de NetScaler Gateway o la utilidad de configuración para configurar el nombre de host de los sitios de SharePoint.

En el asistente de NetScaler Gateway, avance por el asistente para configurar la configuración. Cuando llegue a la página Configurar el acceso sin cliente, escriba la dirección web del sitio de SharePoint y, a continuación, haga clic en **Agregar**.

Para agregar más sitios web o configurar SharePoint por primera vez tras ejecutar el asistente de NetScaler Gateway, utilice la utilidad de configuración.

> **Importante:**
>
> Classic Clientless Access admite versiones anteriores a SharePoint 2013 y OWA 2013. Advanced Clientless Access es compatible con SharePoint 2016 y OWA 2016 y versiones posteriores.

Configurar el acceso sin cliente para SharePoint mediante la interfaz gráfica de usuario de NetScaler

1. **Vaya a** NetScaler Gateway**> Configuración global.**
2. En el panel de detalles, en Acceso sin cliente, haga clic en **Configurar acceso sin cliente para SharePoint**.
3. En Acceso sin cliente para SharePoint, en Nombre de host del servidor de SharePoint, escriba el nombre de host del sitio de SharePoint y, a continuación, haga clic en **Agregar**.
4. Repita el paso 3 para cada sitio de SharePoint que quiera agregar a la lista y, a continuación, haga clic en **Aceptar** cuando haya terminado.

Establecer un sitio de SharePoint como página principal

Si quiere establecer un sitio de SharePoint como página principal de los usuarios, configure un perfil de sesión e introduzca el nombre de host del sitio de SharePoint.

Para configurar un sitio de SharePoint como página principal

1. Vaya a **NetScaler Gateway > Directivas y,** a continuación, haga clic en **Sesión**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.

5. En Nombre , escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, junto a Página principal, haga clic en **Sobrescribir global y,** a continuación, escriba el nombre del sitio de SharePoint.
7. Junto a Acceso sin cliente, haga clic en **Sobrescribir global**, seleccione **Activado y,** a continuación, haga clic en **Crear**.
8. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Después de completar la directiva de sesión, enlaza a usuarios, grupos, servidores virtuales o de forma global. Cuando los usuarios inician sesión, ven el sitio web de SharePoint como su página principal.

Habilitar la resolución de nombres para servidores SharePoint 2007

Los servidores de SharePoint 2007 envían el nombre del servidor configurado como nombre de host dentro de varias URL como parte de la respuesta. Si un nombre de servidor de SharePoint configurado no es el nombre de dominio completo (FQDN), NetScaler Gateway no puede resolver la dirección IP mediante el nombre del servidor de SharePoint y algunas funciones de usuario se agotan con el mensaje de error "HTT:1.1 Tiempo de espera de puerta de enlace". Estas funciones pueden incluir la entrada y salida de archivos, ver el espacio de trabajo y cargar varios archivos cuando los usuarios inician sesión mediante el acceso sin cliente.

Para resolver este problema, puede probar una de las siguientes opciones:

- Configure un sufijo DNS en NetScaler Gateway para que el nombre de host de SharePoint se convierta en un FQDN antes de la resolución de nombres.
- Configure una entrada DNS local en NetScaler Gateway para cada nombre de servidor de SharePoint.
- Cambie todos los nombres de servidor de SharePoint para usar el FQDN, como SharePoint.intranetdomain en lugar de SharePoint.

Configurar un sufijo DNS

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **DNS** y, a continuación, haga clic en **Sufijo DNS**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Sufijo DNS**, escriba el nombre de dominio de la intranet como sufijo, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Puede repetir el paso 3 para cada dominio que quieras agregar.

Para configurar un registro DNS local para cada nombre de servidor de SharePoint en NetScaler Gateway

1. En la utilidad de configuración, en el panel de navegación, expanda **DNS > Registros** y, a continuación, haga clic en **Registros de direcciones**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre de host**, escriba el nombre de host de SharePoint para el registro de direcciones DNS.
4. En **Dirección IP**, escriba la dirección IP del servidor de SharePoint, haga clic en **Agregar**, en **Crear** y, a continuación, en **Cerrar**.

El nombre de host para el que se agrega un registro A no debe tener un registro CNAME. Además, no puede haber registros A duplicados en el dispositivo.

Habilitar cookies persistentes de acceso a VPN sin cliente

March 27, 2024

Las cookies persistentes son necesarias para acceder a determinadas funciones de SharePoint, como abrir y modificar documentos de Microsoft Word, Excel y PowerPoint alojados en el servidor de SharePoint.

Una cookie persistente permanece en el dispositivo del usuario y se envía con cada solicitud HTTP. NetScaler Gateway cifra la cookie persistente antes de enviarla al complemento del dispositivo del usuario y la actualiza periódicamente mientras exista la sesión. La cookie se vuelve obsoleta si finaliza la sesión.

En el asistente de NetScaler Gateway, los administradores pueden habilitar las cookies persistentes de forma global. También puede crear una directiva de sesión para habilitar las cookies persistentes por usuario, grupo o servidor virtual.

Las siguientes opciones están disponibles para las cookies persistentes:

- Permitir habilita las cookies persistentes y los usuarios pueden abrir y modificar documentos de Microsoft almacenados en SharePoint.
- Denegar inhabilita las cookies persistentes y los usuarios no pueden abrir y modificar documentos de Microsoft almacenados en SharePoint.
- Prompt solicita a los usuarios que permitan o rechacen las cookies persistentes durante la sesión.

Las cookies persistentes no son necesarias para el acceso sin cliente si los usuarios no se conectan a SharePoint.

Configurar cookies persistentes para el acceso VPN sin cliente para SharePoint

Puede configurar cookies persistentes para el acceso sin cliente de SharePoint de forma global o como parte de una directiva de sesión.

Para configurar las cookies persistentes de forma global

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración , haga clic en Cambiar la configuración global.
3. En la ficha Experiencia del cliente, junto a Cookies persistentes de acceso sin cliente, seleccione una opción y, a continuación, haga clic en Aceptar.

Para configurar las cookies persistentes como parte de una directiva de sesión

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, junto a Cookies persistentes de acceso sin cliente, haga clic en Supedición global, seleccione una opción y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear directiva de autenticación, junto a Expresiones con nombre, seleccione General, Valor verdadero, haga clic en Agregar expresión, haga clic en Crear y, a continuación, haga clic en Cerrar.

Cliente VPN de Citrix SSO para dispositivos móviles

January 26, 2024

Citrix SSO es el cliente VPN para dispositivos móviles (macOS, iOS e iOS). Citrix SSO proporciona compatibilidad completa con la administración de dispositivos móviles (MDM) en macOS, iOS y Android. Con un servidor MDM, un administrador puede configurar y administrar de forma remota perfiles VPN a nivel de dispositivo y perfiles VPN por aplicación.
Citrix SSO también admite la mayoría de las funciones de uso común.

Referencias

- Cliente Citrix Secure Access
- Clientes VPN de NetScaler Gateway y funciones compatibles

Configurar la página Opciones del cliente

March 27, 2024

Puede configurar NetScaler Gateway para que proporcione a los usuarios varias opciones de inicio de sesión. Al configurar la página de opciones del cliente, los usuarios tienen la opción de iniciar sesión desde una ubicación con las siguientes opciones:

- Cliente Citrix Secure Access para Windows
- Cliente Citrix Secure Access para macOS X
- StoreFront
- Interfaz Web
- Acceso sin cliente

Los usuarios inician sesión en NetScaler Gateway mediante la dirección web del certificado vinculado a NetScaler Gateway o al servidor virtual. Al crear una directiva y un perfil de sesión, puede determinar las opciones de inicio de sesión que reciben los usuarios. Según cómo configure NetScaler Gateway, la página de opciones del cliente muestra hasta tres iconos que representan las siguientes opciones de inicio de sesión:

- Acceso a la red. Cuando los usuarios inician sesión en NetScaler Gateway por primera vez mediante un explorador web y, a continuación, seleccionan Acceso a la red, aparece la página de descarga. Cuando los usuarios hacen clic en Descargar, el complemento se descarga e instala en el dispositivo del usuario. Cuando finaliza la descarga y la instalación, aparece la interfaz de acceso. Si instala una versión más reciente o vuelve a una versión anterior de NetScaler Gateway, el cliente Citrix Secure Access para Windows actualiza o reduce de forma silenciosa a la versión del dispositivo. Si los usuarios se conectan mediante el cliente Citrix Secure Access para Mac, el complemento se actualiza de forma silenciosa si se detecta una nueva versión del dispositivo cuando los usuarios inician sesión. Esta versión del plug-in no baja de forma silenciosa.
- Interfaz web o StoreFront. Si los usuarios seleccionan la Interfaz Web para iniciar sesión, aparece la página Interfaz Web. Los usuarios pueden acceder a sus aplicaciones publicadas o escritorios virtuales. Si los usuarios seleccionan StoreFront para iniciar sesión, Receiver se abre y los usuarios pueden acceder a las aplicaciones y los escritorios.
  Nota: Si configura StoreFront como opción del cliente, las aplicaciones y los escritorios no aparecen en el panel izquierdo de la interfaz de acceso.

- Acceso sin cliente. Si los usuarios seleccionan el acceso sin cliente para iniciar sesión, aparece la interfaz de acceso o la página principal personalizada. En la interfaz de Access, los usuarios pueden desplazarse a recursos compartidos de archivos, sitios web y usar Outlook Web Access.

Secure Browse permite a los usuarios conectarse a través de NetScaler Gateway desde un dispositivo iOS. Si habilita Secure Browse, cuando los usuarios inician sesión con Secure Hub, Secure Browse inhabilita la página de opciones del cliente.

Mostrar la página Opciones del cliente al iniciar sesión

Al habilitar la opción de opciones de cliente, los usuarios pueden iniciar sesión con el cliente Citrix Secure Access, la Interfaz Web, Receiver o acceder sin cliente desde una página web tras una autenticación correcta en NetScaler Gateway. Cuando el inicio de sesión se realiza correctamente, aparecen iconos en la página web desde los que los usuarios pueden elegir el método para establecer una conexión.

Puede habilitar las opciones del cliente sin utilizar el análisis de dispositivos de punto final ni implementar el respaldo de casos de acceso. Si no define una expresión de seguridad del cliente, los usuarios reciben opciones de conexión para la configuración configurada en NetScaler Gateway. Si existe una expresión de seguridad de cliente para la sesión de usuario y el dispositivo de usuario falla el análisis del punto final, la página de opciones solo ofrece la opción de utilizar la Interfaz Web si está configurada. De lo contrario, los usuarios pueden utilizar el acceso sin cliente para iniciar sesión.

Las opciones del cliente se configuran de forma global o mediante un perfil y una directiva de sesión.

> **Importante:**
>
> Al configurar las opciones del cliente, no configure los grupos de cuarentena. Dispositivos de usuario que no superan el análisis de dispositivos de punto final y se ponen en cuarentena y se tratan igual que los dispositivos de usuario que superan el análisis de dispositivos de punto final.

Habilitar opciones de opciones de clientes a nivel

1. En la GUI, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Configuración, haga clic en **Cambiar la configuración global**.
3. En la pestaña Experiencia del cliente, haga clic en **Configuración avanzada** .
4. En la ficha General, haga clic en **Opciones del cliente y,** a continuación, haga clic en **Aceptar**.

Habilitar las opciones del cliente como parte de una directiva de sesión

También puede configurar las opciones de cliente como parte de una directiva de sesión y, a continuación, vincularlas a usuarios, grupos y servidores virtuales.

1. En la GUI, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas y, a continuación,** haga clic en **Sesión**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en **Nuevo** .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha Experiencia del cliente, haga clic en **Avanzado**.
7. En la ficha General, junto a Opciones del cliente, haga clic en **Sobrescribir global**, haga clic en **Opciones del cliente**, en **Aceptar y,**a continuación, en **Crear**.
8. En el cuadro de diálogo Crear directiva de sesión, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Configurar opciones de opciones de cliente

Además de habilitar las opciones del cliente mediante un perfil y una directiva de sesión, debe configurar la configuración del software de usuario. Por ejemplo, desea que los usuarios inicien sesión mediante el cliente Citrix Secure Access, StoreFront o la Interfaz Web, o mediante el acceso sin cliente. Se crea un perfil de sesión que habilita las tres opciones y las opciones del cliente. A continuación, se crea una directiva de sesión con la expresión establecida en valor True con el perfil adjunto. A continuación, vincula la directiva de sesión a un servidor virtual.

Antes de crear la directiva y el perfil de sesión, debe crear un grupo de autorización para los usuarios.

Crear un grupo de autorización

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, **NetScaler Gateway > Administración de usuarios**y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo**, escriba el nombre del grupo.
4. En la ficha **Usuarios**, seleccione los usuarios, haga clic en **Agregar** para cada uno, en **Crear** y, a continuación, en **Cerrar**.

El siguiente procedimiento es un ejemplo de perfil de sesión para las opciones de cliente con el cliente Citrix Secure Access, StoreFront y el acceso sin cliente.

Crear un perfil de sesión para las opciones del cliente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Sesión**.
2. En el panel de detalles, haga clic en la pestaña **Perfiles** y, a continuación, en **Agregar** .
3. En **Nombre**, escriba un nombre para el perfil.
4. En la ficha **Experiencia del cliente**, haga lo siguiente:
    a) Junto a Página de inicio, haga clic en **Supeditación global** y, a continuación, desmarca **Mostrar página de inicio**. Esto inhabilita la interfaz de acceso.
    b) Junto a **Acceso sin cliente**, haga clic en **Supedición global**y, a continuación, selecciona **DESACTIVADO**.
    c) Junto a **Tipo de complemento, haga clic enSupedición global**y, a continuación, seleccione Windows/Mac OS X.
    d) Haga clic en **Configuración avanzada** y, junto a **Opciones del cliente**, haga clic en **Supedición global**y haga clic en **Opciones del cliente**.
5. En la ficha **Seguridad**, junto a **Acción de autorización predeterminada**, haga clic en **Supeditación global** y, a continuación, seleccione **PERMITIR**.
6. En la pestaña **Seguridad** , haz clic en **Configuración avanzada** .
7. En **Grupos de autorización**, haga clic en **Supeditación global**, en **Agregar**y, a continuación, seleccione el grupo.
8. En la ficha **Aplicaciones publicadas**, haga lo siguiente:
    a) Junto a **Proxy ICA**, haga clic en **Supedición global**y, a continuación, selecciona **DESACTIVADO**.
    b) Junto a **Dirección de interfaz web**, haga clic en **Supeditación global**y, a continuación, escriba la dirección web de StoreFront, como. http://ipAddress/Citrix/
    c) Junto a **Modo de portal de Interfaz Web**, haga clic en **Supedición global** y, a continuación, seleccione **COMPACT**.
    d) Junto a **Dominio de inicio de sesión único, haga clic enSupeditación global**y, a continuación, escribe el nombre del dominio.
9. Haga clic en **Crear**y, a continuación, en **Cerrar**.

Si desea utilizar el cliente Citrix Secure Access para Java como opción de cliente, en la ficha **Experiencia del cliente**, en Tipo de complemento, seleccione **Java**. Si selecciona esta opción, debe configurar una aplicación de intranet y establecer el modo de interceptación en Proxy.

Después de crear el perfil de sesión, cree una directiva de sesión. Dentro de la directiva, seleccione el perfil y defina la expresión en Valor verdadero.

Para utilizar StoreFront como opción de cliente, también debe configurar Secure Ticket Authority (STA) en NetScaler Gateway. El STA está enlazado al servidor virtual.

> **Nota:**
>
> Si el servidor que ejecuta StoreFront no está disponible, la opción de Citrix Virtual Apps no aparece en la página de opciones.

Configurar el servidor STA globalmente

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway**y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Servidores, haga clic en Vincular o desvincular los **servidores STA** que utilizará Secure Ticket Authority.
3. En el cuadro de diálogo **Enlazar/desenlazar servidores STA**, haga clic en **Agregar**.
4. En el cuadro de diálogo **Configurar servidor STA**, en URL, escriba la dirección web del servidor STA y, a continuación, haga clic en **Crear**.
5. Repita los pasos 3 y 4 para agregar más servidores STA y, a continuación, haga clic en **Aceptar**.

Enlazar el STA a un servidor virtual

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales**.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha **Aplicaciones publicadas**, en **Secure Ticket Authority**, en **Activo**, seleccione los servidores STA y, a continuación, haga clic en **Aceptar**.

También puede agregar servidores STA en la ficha **Aplicaciones publicadas**.

Configurar reserva de caso de acceso

March 27, 2024

SmartAccess permite a NetScaler Gateway determinar automáticamente los métodos de acceso permitidos para un dispositivo de usuario en función de los resultados de un análisis de puntos finales. El escenario alternativo de acceso amplía aún más esta capacidad al permitir que un dispositivo de usuario pase del cliente Citrix Secure Access a la interfaz web o StoreFront mediante la aplicación Citrix Workspace si el dispositivo de usuario no supera el análisis inicial de endpoint.

Para habilitar el respaldo de casos de acceso, configure una directiva posterior a la autenticación que determina si los usuarios reciben un método de acceso alternativo al iniciar sesión en NetScaler Gateway. Esta directiva posterior a la autenticación se define como una expresión de seguridad del cliente

que se configura de forma global o como parte de un perfil de sesión. Si configura un perfil de sesión, el perfil se asocia a una directiva de sesión que, a continuación, enlaza a usuarios, grupos o servidores virtuales. Al habilitar la opción alternativa de casos de acceso, NetScaler Gateway inicia un análisis de dispositivos de punto final tras la autenticación del usuario. Los resultados de los dispositivos de usuario que no cumplen los requisitos de un análisis posterior a la autenticación de reserva son los siguientes:

- Si las opciones de cliente están habilitadas, los usuarios pueden iniciar sesión en la Interfaz Web o StoreFront mediante únicamente la aplicación Citrix Workspace.
- Si el acceso sin cliente y las opciones de cliente están inhabilitadas, los usuarios se pueden poner en cuarentena en un grupo que proporciona acceso solo a la Interfaz Web o a StoreFront.
- Si el acceso sin cliente y la Interfaz Web o StoreFront están habilitados en NetScaler Gateway y ICA Proxy está inhabilitado, los usuarios recurren al acceso sin cliente.
- Si la Interfaz Web o StoreFront no están configuradas y el acceso sin cliente está configurado para permitir, los usuarios recurren al acceso sin cliente.

Cuando se inhabilita el acceso sin cliente, se debe configurar la siguiente combinación de opciones para la reserva del caso de acceso:

- Defina los parámetros de seguridad del cliente para el análisis posterior a la autenticación de reserva.
- Defina la página de inicio de la Interfaz Web.
- Inhabilitar las opciones del cliente.
- Si los dispositivos de usuario fallan en la comprobación de seguridad del cliente, los usuarios se colocan en un grupo de cuarentena que permite el acceso solo a la Interfaz Web o StoreFront y a las aplicaciones publicadas.

Crear directivas para la suplencia de casos de acceso

Para configurar NetScaler Gateway para la suplencia de casos de acceso, debe crear directivas y grupos de las siguientes maneras:

- Cree un grupo de cuarentena en el que se coloquen los usuarios si se produce un error en la exploración de análisis de dispositivos de punto final.
- Cree una configuración global de Interfaz Web o StoreFront que se utilice si se produce un error en la exploración de análisis de dispositivos de punto final.
- Cree una directiva de sesión que anule la configuración global y, a continuación, vincule la directiva de sesión a un grupo.
- Cree una directiva de seguridad global del cliente que se aplique si se produce un error en el análisis de dispositivos de punto final.

Al configurar el respaldo del caso de acceso, siga las siguientes pautas:

- El uso de opciones de cliente o de respaldo de casos de acceso requiere el complemento Endpoint Analysis para todos los usuarios. Si el análisis de endpoint no se puede ejecutar o si los usuarios seleccionan Omitir exploración durante el análisis, se deniega el acceso a los usuarios.
  Nota: La opción de omitir el análisis se elimina en NetScaler Gateway 10.1, compilación 120.1316.e
- Al habilitar las opciones del cliente, si el dispositivo del usuario no supera el análisis de endpoint, los usuarios se colocan en el grupo de cuarentena. Los usuarios pueden seguir iniciando sesión con el cliente Citrix Secure Access o la aplicación Citrix Workspace en la Interfaz Web o StoreFront.
  Nota: Citrix recomienda no crear un grupo de cuarentena si habilita las opciones del cliente. Los dispositivos de usuario que no superan el análisis de dispositivos de punto final se ponen en cuarentena se tratan del mismo modo que los dispositivos de usuario que superan el análisis de dispositivos de punto final.
- Si se produce un error en el análisis de endpoint y el usuario se coloca en el grupo de cuarentena, las directivas enlazadas al grupo de cuarentena solo serán efectivas si no hay directivas vinculadas directamente al usuario que tengan un número de prioridad igual o inferior que las directivas vinculadas al grupo de cuarentena.
- Puede utilizar distintas direcciones web para la interfaz de acceso y la Interfaz Web o StoreFront. Al configurar las páginas principales, la página principal de la interfaz de acceso tiene prioridad para el cliente Citrix Secure Access y la página principal de la interfaz web tiene prioridad para los usuarios de la interfaz web. La página principal de la aplicación Citrix Workspace tiene prioridad para StoreFront.

Crear un grupo de cuarentena

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios**y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre del grupo**, escriba un nombre para el grupo, haga clic en **Crear y,** a continuación, en **Cerrar**.
   Importante: El nombre del grupo de cuarentena no debe coincidir con el nombre de ningún grupo de dominio al que puedan pertenecer los usuarios. Si el grupo de cuarentena coincide con un nombre de grupo de Active Directory, los usuarios se ponen en cuarentena aunque el dispositivo del usuario supere el análisis de seguridad del análisis de endpoint.

Después de crear el grupo, configure NetScaler Gateway para que vuelva a la Interfaz Web si el dispositivo de usuario no supera la exploración de análisis de endpoint.

Configurar los ajustes para poner en cuarentena las conexiones

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.**
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Aplicaciones publicadas**, junto a **Proxy ICA**, seleccione **DESACTIVADO**.
4. Junto a **Dirección de la interfaz web**, escriba la dirección web de StoreFront o de la interfaz web.
5. Junto a Dominio de **inicio de sesión único, escriba el nombre de su dominio**de Active Directory y, a continuación, haga clic en **Aceptar**.

Después de configurar la configuración global, cree una directiva de sesión que sustituya la configuración global del proxy ICA y, a continuación, vincule la directiva de sesión al grupo de cuarentena.

Crear una directiva de sesión para la suplencia de casos de acceso

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway > Directivas**y, a continuación, haga clic en Sesión.**
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En la ficha **Aplicaciones publicadas**, junto a **Proxy ICA**, haga clic en **Sobrescribir global**, seleccione **Activado y,** a continuación, haga clic en **Crear**.
6. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Después de crear la directiva de sesión, enlaza la directiva a un grupo de cuarentena.

Enlazar la directiva de sesión al grupo de cuarentena

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Administración de usuarios**y, a continuación, haga clic en **Grupos AAA**.
2. En el panel de detalles, seleccione un grupo y, a continuación, haga clic en **Abrir**.
3. Haga clic en Sesión.
4. En la ficha **Directivas**, seleccione **Sesión**y, a continuación, haga clic en **Insertar directiva**.
5. En **Nombre de directiva**, seleccione la directiva y, a continuación, haga clic en **Aceptar**.

Después de crear la directiva de sesión y el perfil que habilita la Interfaz Web o StoreFront en NetScaler Gateway, cree una directiva de seguridad global del cliente.

Crear una directiva de seguridad global para clientes

1. **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.**
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la pestaña **Seguridad** , haz clic en **Configuración avanzada** .
4. En **Seguridad del cliente**, introduzca la expresión. Para obtener más información sobre la configuración de expresiones del sistema, consulte Configuración de expresiones de sistema y Configuración de expresiones de seguridad de cliente compuestas
5. En **Grupo de cuarentena**, seleccione el grupo que configuró en el procedimiento de grupo y, a continuación, haga clic en **Aceptar**.

Configurar las conexiones para el cliente Citrix Secure Access

January 26, 2024

Las conexiones de dispositivos de usuario se configuran definiendo los recursos a los que los usuarios pueden acceder en la red interna. La configuración de conexiones de dispositivos de usuario incluye:

- Definir los dominios a los que se permite el acceso de los usuarios.
- Configuración de direcciones IP para los usuarios, incluidos los grupos de direcciones (IP de intranet).
- Configuración de los ajustes de tiempo de espera.
- Configuración del inicio de sesión único.
- Configuración de la interceptación de clientes.
- Configuración de túneles divididos.
- Configuración de conexiones a través de un servidor proxy.
- Configuración del software de usuario para conectarse a través de NetScaler Gateway.
- Configuración del acceso para dispositivos móviles.

La mayoría de las conexiones de dispositivos de usuario se configuran mediante un perfil que forma parte de una directiva de sesión. También puede definir la configuración de conexión del dispositivo de usuario mediante aplicaciones de intranet, autenticación previa y directivas de tráfico.

> **Nota:**
>
> El plug-in VPN de Windows y los plug-ins EPA recopilan datos de telemetría para sus distintas operaciones. Para inhabilitar la funcionalidad, haga lo siguiente en la máquina cliente.
>
> Establezca el registro “HKLM\Software\Citrix\Secure Access Client\DisableGA”del tipo

> REG_DWORD en 1.

Configurar el número de sesiones de usuario

March 27, 2024

Puede configurar el número máximo de usuarios a los que se les permite conectarse a NetScaler Gateway en un momento determinado, ya sea a nivel global o a nivel de servidor virtual. Las sesiones no se crean en NetScaler Gateway cuando el número de usuarios que se conectan al dispositivo supera el valor configurado. Si el número de usuarios supera el número permitido, los usuarios reciben un mensaje de error.

Para establecer el límite global de usuarios

Al configurar el límite de usuarios de forma global, la restricción se aplica a todos los usuarios que establecen sesiones en distintos servidores virtuales del sistema. Cuando el número de sesiones de usuario alcanza el valor establecido, no se pueden establecer nuevas sesiones en ningún servidor virtual presente en NetScaler Gateway.

Establece el número máximo de usuarios a nivel global al establecer el tipo de autenticación predeterminado para NetScaler Gateway.

1. En la utilidad de configuración, en la pestaña Configuración , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración global.
2. En el panel de detalles, en Configuración, haga clic en Cambiar la configuración de autenticación.
3. En el cuadro de diálogo Configuración de autenticación global, en Número máximo de usuarios, escriba el número de usuarios y, a continuación, haga clic en Aceptar.

Para establecer el límite de usuarios por servidor virtual

También puede aplicar el límite de usuarios a cada servidor virtual del sistema. Al configurar el límite de usuario por servidor virtual, la restricción se aplica solo a los usuarios que establecen sesiones con el servidor virtual concreto. Los usuarios que establecen sesiones con otros servidores virtuales no se ven afectados por este límite.

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Servidores virtuales.
2. En el panel de detalles, haga clic en un servidor virtual y, a continuación, en Abrir .
3. En Usuarios máximos, escriba el número de usuarios y, a continuación, haga clic en Aceptar.

Configurar ajustes de tiempo de espera

March 27, 2024

Puede configurar NetScaler Gateway para forzar una desconexión si no hay actividad en la conexión durante un número de minutos especificado. Un minuto antes de que se acabe el tiempo de espera de una sesión (se desconecte), el usuario recibe una alerta que indica que la sesión se cierra. Si la sesión se cierra, el usuario debe volver a iniciar sesión.

Las siguientes opciones de tiempo de espera están disponibles.

- **Tiempo muerto forzado.** Si habilita esta configuración, NetScaler Gateway desconecta la sesión una vez transcurrido el intervalo de tiempo de espera, independientemente de lo que esté haciendo el usuario. El usuario no puede realizar ninguna acción para evitar que se produzca la desconexión cuando transcurra el intervalo de tiempo de espera. Esta configuración se aplica a los usuarios que se conectan con el cliente Citrix Secure Access, la aplicación Citrix Workspace, Secure Hub o mediante un navegador web. El valor mínimo es 1 y el valor máximo es 65535.
- **Tiempo de espera de sesión.** Si habilita esta configuración, NetScaler Gateway desconecta la sesión si no se detecta actividad de red durante el intervalo especificado. Esta configuración se aplica a los usuarios que se conectan con el cliente Citrix Secure Access, la aplicación Citrix Workspace, Citrix Secure Hub o mediante un navegador web. El tiempo de espera predeterminado es de 30 minutos. El valor mínimo es 1 y el valor máximo es 65535.
- Tiempo de**espera de la sesión inactiva.** Duración tras la cual el cliente Citrix Secure Access finaliza una sesión inactiva si no hay actividad del usuario, por ejemplo, con el ratón, el teclado o el toque durante el intervalo especificado. Esta configuración se aplica únicamente a los usuarios que se conectan con el cliente Citrix Secure Access. El valor mínimo es 1 y el valor máximo es 9999.

Puede habilitar cualquiera de los ajustes de tiempo de espera introduciendo un valor entre 1 y 65536 para especificar los minutos del intervalo de tiempo de espera. Si habilita más de una de estas configuraciones, el primer intervalo de tiempo de espera que transcurriera cierra la conexión del dispositivo del usuario.

La configuración del tiempo de espera se establece mediante la configuración global o mediante un perfil de sesión. Al agregar el perfil a una directiva de sesión, la directiva se envuelve a un usuario, grupo o servidor virtual. Al configurar la configuración del tiempo de espera de forma global, la configuración se aplica a todas las sesiones de usuario.

> **Nota:**
>
> - En Siempre activado (modo servicio o modo usuario), el cliente VPN ignora todos los tiem-

> pos de espera. Las decisiones de tiempo de espera forzado y de tiempo de espera de sesión se producen en el dispositivo NetScaler y, por lo tanto, esos tiempos de espera funcionan según lo previsto. Si se agota el tiempo de espera, el complemento VPN intenta realizar la autenticación automática.
>
> En Always On, dado que el dispositivo del usuario debe estar conectado a través del túnel VPN todo el tiempo, no configure el tiempo de espera forzado ni el tiempo de espera inactivo del cliente. Sin embargo, el tiempo de espera de la sesión se puede configurar para eliminar las sesiones obsoletas.
>
> - Algunas aplicaciones, como Microsoft Outlook, envían automáticamente sondeos de tráfico de red a servidores de correo electrónico sin intervención del usuario. Citrix recomienda configurar el tiempo de espera de la sesión inactiva con el tiempo de espera de la sesión para garantizar que una sesión que se deja desatendida en un dispositivo de usuario caduque en un tiempo razonable.

Configurar tiempos de espera forzados

Un tiempo de espera forzado desconecta automáticamente el cliente Citrix Secure Access después de un período de tiempo especificado. Puede configurar un tiempo de espera forzado de forma global o como parte de una directiva de sesión.

Configurar un tiempo de espera forzado global

1. En la utilidad de configuración, en la pestaña **Configuración** , en el panel de navegación, expanda NetScaler Gateway y, a continuación, haga clic en Configuración **global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Configuración de red**, haga clic en **Configuración avanzada**.
4. En Tiempo de espera forzado (minutos), escriba el número de minutos que los usuarios pueden permanecer conectados.
5. En Advertencia de tiempo de espera forzado (minutos), escriba el número de minutos antes de que se avise a los usuarios de que la conexión se va a desconectar y, a continuación, haga clic en **Aceptar**.

Configurar un tiempo de espera forzado en una directiva de sesión

Si quiere tener más control sobre quién recibe el tiempo de espera forzado, cree una directiva de sesión y, a continuación, aplíquela a un usuario o grupo.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**.

2. En el panel de detalles, haga clic en **Agregar**.
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en **Nuevo** .
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha **Configuración de red**, haga clic en **Avanzadas**.
7. En Tiempos de espera, haga clic en **Supeditar global** y, en Tiempo de espera forzado (minutos), escriba el número de minutos que los usuarios pueden permanecer conectados.
8. Junto a **Advertencia de tiempo de espera forzado (minutos)**, haga clic en **Supeditación global e introduzca** el número de minutos durante los que se avisa a los usuarios de que la conexión se va a desconectar. Haga clic en **Aceptar** dos veces.
9. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione General, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Configurar los tiempos de espera de sesión o de inactividad

Puede utilizar la GUI de NetScaler para configurar los valores de tiempo de espera de sesión y cliente de forma global o para crear una directiva de sesión. Al crear un perfil y una directiva de sesión, establezca la expresión en True.

> **Nota:**
>
> Si no supedita explícitamente la configuración global y establece el tiempo de espera de la sesión en **Experiencia de cliente > Tiempo de espera de sesión (minutos)**, esto puede provocar bucles de autenticación que requieran volver a iniciar sesión. Esto ocurre incluso con el tiempo de espera predeterminado de la sesión de 30 minutos.

Para configurar el tiempo de espera por inactividad de una sesión o cliente de forma global mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, realice una o ambas de las acciones siguientes:
   - En Tiempo de **espera de sesión (minutos)**, escriba el número de minutos.
   - En Tiempo de **espera inactivo del cliente (minutos)**, escriba el número de minutos y, a continuación, haga clic en **Aceptar**.

Para configurar la configuración del tiempo de espera por inactividad de la sesión o del cliente mediante una directiva de sesión mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** > **Directivas** y, a continuación, haga clic en **Sesión**
2. En la página **Perfiles y directivas de sesión de NetScaler Gateway**, haga clic en **Perfiles de sesión**y, a continuación, haga clic en **Agregar**.
3. En Nombre , escriba un nombre para el perfil.
4. En la ficha **Experiencia del cliente**, realice una o ambas de las acciones siguientes:
    - Junto a Tiempo de **espera de sesión (minutos)**, haga clic en **Supedición global** y, a continuación, escriba el número de minutos y, a continuación, haga clic en **Crear**.
    - Junto a Tiempo de **espera inactivo del cliente (minutos)**, haga clic en **Supedición global**, escriba el número de minutos y, a continuación, haga clic en **Crear**.
5. a) En la página **Perfiles y directivas de sesión de NetScaler Gateway**, haga clic en **Directivas de sesión**y, a continuación, en **Agregar**.
6. En la **directiva Crear sesión de NetScaler Gateway**,
    - En **Nombre**, introduzca el nombre de la directiva.
    - En **Perfil**, seleccione el perfil que especifica la acción que aplicará la nueva directiva de sesión si se cumplen los criterios de la regla.
    - seleccione **Directiva avanzada**.
    - En el campo **Expresión**, agregue la expresión o el nombre de una expresión con nombre y especifique el tráfico que coincide con la directiva.
    - Haga clic en **Crear**y, a continuación, en **Cerrar**.

Conéctese a los recursos de red interna

January 26, 2024

Puede configurar NetScaler Gateway para que los usuarios puedan acceder a los recursos de la red interna. Si inhabilita la tunelización dividida, todo el tráfico de red del dispositivo de usuario se envía a NetScaler Gateway y las directivas de autorización determinan si el tráfico puede pasar a través de recursos de red internos. Cuando habilita el túnel dividido, solo el tráfico destinado a la red interna es interceptado por el dispositivo del usuario y enviado a NetScaler Gateway. Puede configurar qué direcciones IP intercepta NetScaler Gateway mediante aplicaciones de intranet.

Si utiliza el cliente Citrix Secure Access para Windows, defina el modo de intercepción en transparente. Si utiliza el cliente Citrix Secure Access para Java, defina el modo de intercepción como proxy. Si

establece el modo de interceptación en transparente, puede permitir el acceso a los recursos de red mediante:

- Una única dirección IP y máscara de subred
- Una serie de direcciones IP

Si establece el modo de interceptación en proxy, puede configurar las direcciones IP de destino y origen y los números de puerto.

Configurar el acceso de red a los recursos de red internos

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda NetScaler Gateway, Recursos y, a continuación, haga clic en **Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. Complete los parámetros para permitir el acceso a la red, haga clic en **Crear** y, a continuación, en **Cerrar.**

Configurar túnel dividido

March 27, 2024

Puede habilitar la tunelización dividida para evitar que el cliente Citrix Secure Access envíe tráfico de red innecesario a NetScaler Gateway.

Cuando no habilita la tunelización dividida, el cliente Citrix Secure Access captura todo el tráfico de red que se origina en un dispositivo de usuario y lo envía a través del túnel VPN a NetScaler Gateway.

Si habilita la tunelización dividida, el cliente Citrix Secure Access envía solo el tráfico destinado a las redes protegidas por NetScaler Gateway a través del túnel VPN. El cliente Citrix Secure Access no envía el tráfico de red destinado a redes desprotegidas a NetScaler Gateway.

Cuando se inicia el cliente Citrix Secure Access, obtiene la lista de aplicaciones de intranet de NetScaler Gateway. El cliente Citrix Secure Access examina todos los paquetes transmitidos en la red desde el dispositivo de usuario y compara las direcciones de los paquetes con la lista de aplicaciones de intranet. Si la dirección de destino del paquete se encuentra dentro de una de las aplicaciones de la intranet, el cliente Citrix Secure Access envía el paquete a través del túnel VPN a NetScaler Gateway. Si la dirección de destino no se encuentra en una aplicación de intranet definida, el paquete no se cifra y el dispositivo del usuario enruta el paquete de forma adecuada. Al habilitar la tunelización dividida, las aplicaciones de intranet definen el tráfico de red que se intercepta.

> **Nota:**
>
> Si los usuarios se conectan a aplicaciones publicadas en un conjunto de servidores mediante la aplicación Citrix Workspace, no es necesario configurar la tunelización dividida.

NetScaler Gateway también admite la tunelización dividida inversa, que define el tráfico de red que NetScaler Gateway no intercepta. Si establece la tunelización dividida como inversa, las aplicaciones de intranet definen el tráfico de red que NetScaler Gateway no intercepta. Cuando habilita la tunelización dividida inversa, todo el tráfico de red dirigido a direcciones IP internas omite el túnel VPN, mientras que el resto del tráfico pasa por NetScaler Gateway. La tunelización dividida inversa se puede utilizar para registrar todo el tráfico LAN no local. Por ejemplo, si los usuarios tienen una red inalámbrica doméstica y han iniciado sesión con el cliente Citrix Secure Access, NetScaler Gateway no intercepta el tráfico de red destinado a una impresora u otro dispositivo de la red inalámbrica.

Para obtener más información sobre las aplicaciones de intranet, consulte Configuración de la interceptación de clientes.

Configure la tunelización dividida como parte de la directiva de sesión.

Para configurar el túnel dividido

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **Políticas de NetScaler Gateway** y, a continuación, haga clic en **Sesión.**
2. En el panel de detalles, en la ficha **Perfiles**, seleccione un perfil y, a continuación, haga clic en **Abrir.**
3. En la ficha **Experiencia del cliente**, junto a **Dividir túnel**, seleccione **Anulación global**, seleccione una opción y, a continuación, haga clic dos veces en **Aceptar**.

Configurar la autorización y la tunelización dividida

Al planificar la implementación de NetScaler Gateway, es importante tener en cuenta la tunelización dividida y la acción de autorización y las directivas de autorización predeterminadas.

Por ejemplo, tiene una directiva de autorización que permite el acceso a un recurso de red. La tunelización dividida está activada y no configura las aplicaciones de intranet para enviar tráfico de red a través de NetScaler Gateway. Cuando NetScaler Gateway tiene este tipo de configuración, se permite el acceso al recurso, pero los usuarios no pueden acceder al recurso.

Si la directiva de autorización niega el acceso a un recurso de red, tiene los túneles divididos configurados en ON y las aplicaciones de intranet están configuradas para enrutar el tráfico de red a través de NetScaler Gateway. El cliente Citrix Secure Access envía el tráfico a NetScaler Gateway, pero se deniega el acceso al recurso.

Para obtener más información sobre las opciones de tunelización dividida, consulte Opciones de tunelización dividida.

Configurar la interceptación de clientes

March 27, 2024

Las reglas de interceptación para las conexiones de usuario en NetScaler Gateway se configuran mediante aplicaciones de intranet. De forma predeterminada, cuando configura la dirección IP del sistema, una dirección IP asignada o una dirección IP de subred en el dispositivo, las rutas de subred se crean en función de estas direcciones IP. Las aplicaciones de intranet se crean automáticamente en función de estas rutas y se pueden enlazar a un servidor virtual. Si habilita la tunelización dividida, debe definir aplicaciones de intranet para que se produzca la interceptación de clientes.

Puede configurar las aplicaciones de la intranet mediante la interfaz gráfica de usuario. Puede enlazar aplicaciones de intranet a usuarios, grupos o servidores virtuales.

Si habilita la tunelización dividida y los usuarios se conectan mediante WorxWeb o WorxMail, al configurar la interceptación de clientes, debe agregar las direcciones IP de Citrix Endpoint Management y del servidor Exchange. Si no habilita la tunelización dividida, no es necesario configurar las direcciones IP de Endpoint Management y Exchange en aplicaciones de intranet.

Para obtener información sobre la configuración de túneles divididos, consulte Configurar túneles divididos.

Configurar aplicaciones de intranet para el cliente Citrix Secure Access

Para crear aplicaciones de intranet para el acceso de los usuarios a los recursos, defina lo siguiente:

- Una dirección IP
- Una serie de direcciones IP
- Un nombre de host

Al definir una aplicación de intranet en NetScaler Gateway, el cliente Citrix Secure Access para Windows intercepta el tráfico de usuarios destinado al recurso y lo envía a través de NetScaler Gateway.

Al configurar aplicaciones de intranet, tenga en cuenta lo siguiente:

- Cuando Túnel dividido está ACTIVADO,
  - Configure las aplicaciones de la intranet.
  - Asigne aplicaciones de intranet a cada grupo de autenticación, autorización y auditoría.

- Cuando Túnel dividido está DESACTIVADO,
  - Todo el tráfico se intercepta a través del túnel VPN.
  - No es necesario configurar las aplicaciones de intranet.
- Cuando Túnel dividido es INVERSO,
  - Configure las aplicaciones de la intranet. El tráfico que no especifican las aplicaciones de la intranet pasa por el túnel VPN.
  - Asigne las aplicaciones de intranet que se excluirán de la VPN a cada grupo de autenticación, autorización y auditoría.

> **Importante:**
>
> La intercepción debe configurarse en **TRANSPARENTE** independientemente de la configuración del túnel dividido.

Nota:

- Al configurar una aplicación de intranet, debe seleccionar un modo de interceptación que se corresponda con el tipo de software de plug-in utilizado para establecer conexiones.
- No puede configurar una aplicación de intranet tanto para la intercepción proxy como para la transparente.

Para crear una aplicación de intranet para una dirección IP

1. **En la ficha Configuración, en el panel de navegación, expanda**Recursos de NetScaler Gateway**y, a continuación, haga clic en Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En Nombre , escriba un nombre para el perfil.
4. En el cuadro de diálogo **Crear aplicación de intranet** , seleccione **TRANSPARENTE .**
5. En **Tipo de destino** , seleccione **Dirección IP** y máscara de red **.**
6. En Protocolo, seleccione el protocolo que se aplica al recurso de red.
7. En **Dirección IP**, escriba la dirección IP.
8. En **Máscara de red**, escriba máscara de subred, haga clic en **Crear** y, a continuación, haga clic en **Cerrar.**

Para configurar un intervalo de direcciones IP

Si tiene varios servidores en la red, como la web, el correo electrónico y los recursos compartidos de archivos, puede configurar un recurso de red que incluya el rango de IP de los recursos de red. Esta configuración permite a los usuarios acceder a los recursos de red incluidos en el intervalo de direcciones IP.

1. En la pestaña **Configuración** , en el panel de navegación, expanda **Recursos de NetScaler Gateway** y, a continuación, haga clic en **Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre**, escriba un nombre para el perfil.
4. En Protocolo, seleccione el protocolo que se aplica al recurso de red.
5. En el cuadro de diálogo **Crear aplicación de intranet**, seleccione **TRANSPARENTE**.
6. En **Tipo de destino**, seleccione **Intervalo de direcciones IP.**
7. En **Inicio IP**, escriba la dirección IP inicial y, en Fin IP, escriba la dirección IP final, haga clic en **Crear** y, a continuación, haga clic en **Cerrar.**

Para crear una aplicación de intranet para un nombre de host

1. **En la ficha Configuración, en el panel de navegación, expanda**Recursos de NetScaler Gateway**y, a continuación, haga clic en Aplicaciones de intranet.**
2. En el panel de detalles, haga clic en **Agregar.**
3. En **Nombre**, escriba un nombre para el perfil.
4. En el cuadro de diálogo **Crear aplicación de intranet** , seleccione **TRANSPARENTE .**
5. En **Tipo de destino**, seleccione **nombre de host**.
6. En Protocolo, seleccione **CUALQUIERA**, haga clic en **Crear y,** a continuación, haga clic en **Cerrar.**

> **Importante:**
>
> - A partir de la versión 13.0, versión 36.27 y posteriores, el plug-in de la VPN de Windows admite reglas basadas en nombres de host (FQDN) para la tunelización dividida. Debe actualizar tanto el dispositivo NetScaler como el plug-in de la VPN para Windows a la versión 13.0 compilación 36.27 o posterior.
> - También se admiten nombres de host comodín. Por ejemplo, si se configura una aplicación de intranet con el nombre de host "*.ejemplo.com", `a1.example.com`, `b2.example.com` y así sucesivamente.
> - La aplicación de intranet basada en nombres de host solo funciona cuando la tunelización dividida está configurada en ACTIVADO o INVERSO.

Configurar resolución de servicios de nombres

January 26, 2024

Durante la instalación de NetScaler Gateway, puede utilizar el asistente de NetScaler Gateway para configurar otras opciones, incluidos los proveedores de servicios de nombres. Los proveedores de

servicios de nombres traducen el nombre de dominio completo (FQDN) en una dirección IP. En el asistente de NetScaler Gateway, puede configurar un servidor DNS o WINS, establecer la prioridad de la búsqueda DNS y el número de veces que se debe volver a intentar la conexión con el servidor.

Al ejecutar el asistente de NetScaler Gateway, puede agregar un servidor DNS. Puede agregar más servidores DNS y un servidor WINS a NetScaler Gateway mediante un perfil de sesión. A continuación, puede indicar a los usuarios y grupos que se conecten a un servidor de resolución de nombres distinto del que utilizó originalmente el asistente para configurar.

Antes de configurar un servidor DNS adicional en NetScaler Gateway, cree un servidor virtual que actúe como servidor DNS para la resolución de nombres.

Agregar un servidor DNS o WINS dentro de un perfil de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Directivas de NetScaler Gateway** y, a continuación, haga clic en **Sesión.**
2. En el panel de detalles, en la ficha Perfiles, seleccione un perfil y, a continuación, haga clic en Abrir.
3. En la ficha Configuración de red, realice una de las siguientes acciones:
    - Para configurar un servidor DNS, junto a Servidor virtual DNS, haga clic en **Supeditación global**, seleccione el servidor y, a continuación, haga clic en **Aceptar**.
    - Para configurar un servidor WINS, junto a IP del servidor WINS, haga clic en **Supeditación global**, escriba la dirección IP y, a continuación, haga clic en **Aceptar**.

> **Importante:**
>
> Las directivas de respuesta no se evalúan para servidores virtuales DNS no direccionables conectados al perfil de sesión VPN.

Habilitar compatibilidad con proxy para conexiones de usuario

March 27, 2024

Los dispositivos de usuario se pueden conectar a través de un servidor proxy para acceder a redes internas. NetScaler Gateway admite los protocolos HTTP, SSL, FTP y SOCKS. Para habilitar la compatibilidad con proxy para las conexiones de usuario, especifique la configuración en NetScaler Gateway. Puede especificar la dirección IP y el puerto que utiliza el servidor proxy de NetScaler Gateway. El servidor proxy se utiliza como proxy de reenvío para todas las demás conexiones a la red interna.

Configuración de proxy

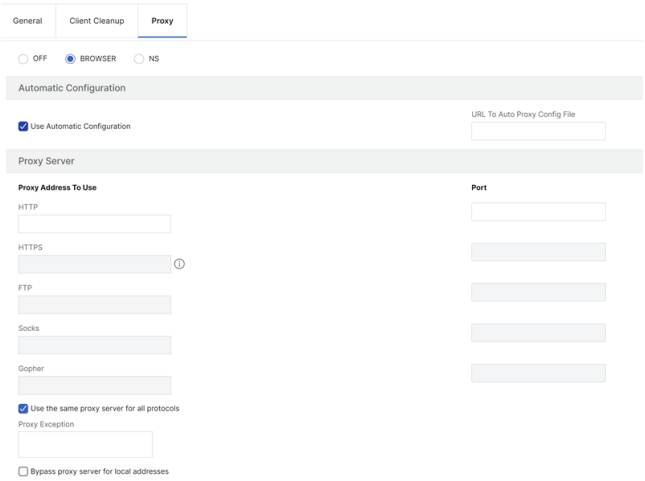
Puede configurar la configuración del proxy en el explorador o en el dispositivo NetScaler. Para configurar la configuración del proxy en el explorador o el dispositivo, vaya a **Configuración global de NetScaler Gateway > ficha Experiencia del cliente > Configuración avanzada > Proxy**y, a continuación, seleccione **Explorador** o **NS**, según corresponda.

- **Explorador**: Cuando elige configurar los ajustes del proxy en el explorador, puede utilizar la opción de configuración automática proporcionando un enlace al archivo de configuración automática del proxy. La configuración automática podría sobrescribir la configuración manual.

  Además, al seleccionar **Browser**, puede omitir los proxies configurados previamente seleccionando la opción de excepción de proxy.

  Nota: Los diferentes tipos de clientes tienen capacidades diferentes en cuanto a la configuración **del proxy del explorador**. Para obtener más información, consulte Clientes VPN de NetScaler Gateway y funciones compatibles.

- **NS**: No puede utilizar la opción de configuración automática si configura la configuración del proxy en el dispositivo NetScaler. No se pueden omitir los proxies configurados previamente cuando configura la configuración del proxy en el dispositivo.



Para configurar la compatibilidad de proxy para conexiones de usuario

1. **En el panel de navegación, expanda**NetScaler Gateway**y, a continuación, haga clic en Configuración global.**
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la pestaña Experiencia del cliente, haga clic en **Configuración avanzada** .
4. En la **ficha Proxy**, en **Configuración de proxy**, seleccione **Navegador.**

5. Para los protocolos, escriba la dirección IP y el número de puerto y, a continuación, haga clic en **Aceptar.**

> **Nota:**
>
> - Si selecciona **NS**, puede configurar servidores proxy que admitan únicamente conexiones HTTP seguras y no seguras.
> - Después de habilitar la compatibilidad con proxy en NetScaler Gateway, especifique los detalles de configuración del dispositivo de usuario del servidor proxy correspondiente al protocolo.
>
>   Después de habilitar la compatibilidad con proxy, NetScaler Gateway envía los detalles del servidor proxy al explorador web del cliente y cambia la configuración del proxy en el explorador.
>
>   – When the user device connects to NetScaler Gateway, the user device can communicate with the proxy server directly for connection to the user's network.
>   – When the user device disconnects from NetScaler Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

Para configurar un servidor proxy para que use todos los protocolos de NetScaler Gateway

Puede configurar un servidor proxy para que admita todos los protocolos que utiliza NetScaler Gateway. Esta configuración proporciona una combinación de dirección IP y puerto para todos los protocolos.

1. En el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada.**
4. En la pestaña **Proxy** , en **Configuración** de proxy , selecciona **Navegador.**
5. Para los protocolos, escriba la dirección IP y el número de puerto.
6. Haga clic en Usar el mismo servidor proxy para todos los protocolos y, a continuación, haga clic en **Aceptar.**

Cuando inhabilita la tunelización dividida y establece toda la configuración del proxy en Activado, la configuración del proxy se propaga a los dispositivos del usuario. Si la configuración del proxy se establece en Equipo, la configuración no se propaga a los dispositivos de usuario.

NetScaler Gateway establece conexiones con el servidor proxy en nombre del dispositivo del usuario.

La configuración del proxy no se propaga al explorador del usuario, por lo que no es posible la comunicación directa entre el dispositivo del usuario y el servidor proxy.

Para configurar NetScaler Gateway para que sea un servidor proxy

Al configurar NetScaler Gateway como servidor proxy, HTTP no seguro y seguro es el único protocolo compatible.

1. **En el panel de navegación, expanda**NetScaler Gateway**y, a continuación, haga clic en Configuración global.**
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada.**
4. En la ficha **Proxy**, en **Configuración del proxy**, seleccione **NS**.
5. Para los protocolos, escriba la dirección IP y el número de puerto y, a continuación, haga clic en **Aceptar.**

Configurar grupos de direcciones

March 27, 2024

En algunas situaciones, los usuarios que se conectan con el cliente Citrix Secure Access necesitan una dirección IP única para NetScaler Gateway. Por ejemplo, en un entorno Samba, cada usuario que se conecta a una unidad de red asignada debe parecer originario de una dirección IP diferente. Al habilitar los grupos de direcciones (también conocidos como agrupación de IP) para un grupo, NetScaler Gateway puede asignar un alias de dirección IP único a cada usuario.

Los grupos de direcciones se configuran mediante direcciones IP de intranet. Es posible que los siguientes tipos de aplicaciones necesiten utilizar una dirección IP única que se extrae del grupo de direcciones IP:

- Voz sobre IP
- FTP activo
- Mensajería instantánea
- Shell seguro (SSH)
- Informática de red virtual (VNC) para conectarse al escritorio de un equipo
- Escritorio remoto (RDP) para conectarse a un escritorio cliente

Puede configurar NetScaler Gateway para asignar una dirección IP interna a los usuarios que se conectan a NetScaler Gateway. Las direcciones IP estáticas se pueden asignar a los usuarios o se puede asignar un rango de direcciones IP a un grupo, servidor virtual o al sistema de forma global.

NetScaler Gateway permite asignar direcciones IP de la red interna a los usuarios remotos. Una dirección IP de la red interna puede dirigirse a un usuario remoto. Si elige utilizar un rango de direcciones IP, el sistema asigna dinámicamente una dirección IP de ese rango a un usuario remoto a petición.

Al configurar grupos de direcciones, tenga en cuenta lo siguiente:

- Las direcciones IP asignadas deben redirigirse correctamente. Para garantizar la redirección correcta, tenga en cuenta lo siguiente:
  - Si no habilita la tunelización dividida, asegúrese de que las direcciones IP se puedan redirigir a través de dispositivos de traducción de direcciones de red (NAT).
  - Todos los servidores a los que se accede mediante conexiones de usuario con direcciones IP de intranet deben tener las puertas de enlace adecuadas configuradas para llegar a esas redes.
  - Configure puertas de enlace o una ruta estática en NetScaler Gateway para que el tráfico de red del software de usuario se enrute a la red interna.
- Solo se pueden utilizar máscaras de subred contiguas al asignar rangos de direcciones IP. Se puede asignar un subconjunto de un rango a una entidad de nivel inferior. Por ejemplo, si un intervalo de direcciones IP está enlazado a un servidor virtual, vincule un subconjunto del rango a un grupo.
- Los intervalos de direcciones IP no se pueden enlazar a varias entidades dentro de un nivel de enlace. Por ejemplo, un subconjunto de un intervalo de direcciones enlazado a un grupo no se puede enlazar a un segundo grupo.
- NetScaler Gateway no permite quitar ni desvincular direcciones IP mientras las utiliza activamente una sesión de usuario.
- Las direcciones IP de la red interna se asignan a los usuarios mediante la siguiente jerarquía:
  - Enlace directo del usuario
  - Grupo de direcciones asignadas
  - Grupo de direcciones asignadas a servidores virtuales
  - Rango global de direcciones
- Solo se pueden utilizar máscaras de subred contiguas para asignar rangos de direcciones. Sin embargo, un subconjunto de un rango asignado podría asignarse a una entidad de nivel inferior. Un intervalo de direcciones globales enlazado puede tener un rango vinculado a lo siguiente:
  - Servidor virtual
  - Grupo
  - Usuario
- Un intervalo de direcciones de servidor virtual enlazado puede tener un subconjunto enlazado a lo siguiente:
  - Grupo

- Usuario

Un intervalo de direcciones de grupo enlazado puede tener un subconjunto enlazado a un usuario.

Cuando se asigna una dirección IP a un usuario, la dirección se reserva para el próximo inicio de sesión del usuario hasta que se agote el intervalo del grupo de direcciones. Cuando se agotan las direcciones, NetScaler Gateway recupera la dirección IP del usuario que más tiempo ha desconectado de NetScaler Gateway.

Si no se puede recuperar una dirección y todas las direcciones están en uso activo, NetScaler Gateway no permite que el usuario inicie sesión. Puede evitar esta situación permitiendo que NetScaler Gateway utilice la dirección IP asignada como dirección IP de intranet cuando el resto de direcciones IP no estén disponibles.

Registro DNS IP de intranet

Si se asigna una IP de intranet a un equipo cliente y después del establecimiento del túnel VIP, el complemento VPN comprueba si esa máquina cliente está unida a un dominio. Si la máquina cliente es una máquina unida a un dominio, el complemento VPN inicia el proceso de registro de DNS para vincular la intranet del nombre de host de la máquina con la dirección IP de intranet asignada. Este registro se revierte antes de la retirada del túnel.

Para que el registro DNS se realice correctamente, asegúrese de que los siguientes botones `nsapimgr`estén configurados. Asegúrese también de que el servidor DNS autoritativo esté configurado para permitir actualizaciones de DNS "no seguras".

- **`nsapimgr` -ys enable_vpn_dns_override=1**: Este indicador se envía al cliente VPN de NetScaler Gateway junto con los demás parámetros de configuración. Si este indicador no está configurado y cuando el cliente VPN intercepta una solicitud de DNS/WINS, envía la correspondiente solicitud HTTP "GET /DNS"al servidor virtual de NetScaler Gateway a través del túnel para obtener la dirección IP resuelta. Sin embargo, si se establece el indicador "enable_vpn_dnstruncate_fix", el cliente VPN reenvía las solicitudes de DNS/WINS de forma transparente al servidor virtual de NetScaler Gateway. En este caso, el paquete DNS se envía tal cual al servidor virtual de NetScaler Gateway a través del túnel VPN. Esto ayuda en los casos en que los registros DNS procedentes de los servidores de nombres configurados en NetScaler Gateway son enormes y no caben en el paquete de respuesta UPD. En este caso, cuando el cliente vuelve a usar TCP-DNS, este paquete TCP-DNS llega al servidor de NetScaler Gateway tal cual y, por lo tanto, el servidor de NetScaler Gateway realiza una consulta TCP-DNS a un servidor DNS.
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**: Este indicador lo utiliza el propio servidor de NetScaler Gateway. Si se establece este indicador, NetScaler Gateway supedita el destino de las "conexiones TCP en el puerto DNS"a los servidores DNS configurados en NetScaler Gateway (en

lugar de intentar enviarlas a la IP del servidor DNS originalmente presente en el paquete TCP-DNS entrante). Para las solicitudes DNS UDP, el valor predeterminado es utilizar los servidores DNS configurados para la resolución DNS. El complemento de NetScaler Gateway para Windows admite actualizaciones de DNS seguras y no seguras. La compatibilidad con la actualización de DNS segura existe de forma predeterminada en las compilaciones 21.7.1.1 o posteriores.

La actualización segura de DNS en el plug-in de Windows está inhabilitada de forma predeterminada. Para habilitarlo, cree un valor de tipo REG_DWORD en `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access`y configúrelo en 1.

- Al establecer el valor en 1, el plug-in de VPN intenta primero la actualización de DNS no segura. Si la actualización de DNS no segura falla, el plug-in de VPN intenta realizar la actualización de DNS segura.
- Para probar solo la actualización segura de DNS, puede establecer el valor en 2.

Para obtener más información sobre cómo configurar estos mandos, consulte.https://support.citrix.com/article/CTX200243

Configurar grupos de direcciones para un usuario, grupo o servidor virtual

1. En la utilidad de configuración, en el panel de navegación, expanda **NetScaler Gateway**y realice una de las siguientes acciones:
   - **Amplíe Administración de usuarios de NetScaler Gateway y, a continuación, haga clic en Usuarios AAA.**
   - **Amplíe**NetScaler Gateway**>**Administración de usuarios**y, a continuación, haga clic en Grupos AAA.**
   - **Amplíe**NetScaler Gateway**y, a continuación, haga clic en Servidores virtuales.**
2. En el panel de detalles, haga clic en un usuario, grupo o servidor virtual y, a continuación, haga clic en **Abrir**.
3. En la ficha IP **de intranet**, en Dirección IP y máscara de red, escriba la dirección IP y la máscara de subred y, a continuación, haga clic en **Agregar**.
4. Repita el paso 3 para cada dirección IP que quiera agregar al grupo y, a continuación, haga clic en **Aceptar**.

Configurar grupos de direcciones de forma global

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.

2. En el panel de detalles, en **IP de intranet**, haga clic en Para asignar una dirección IP estática única o un grupo de direcciones IP para que las usen todas las sesiones de cliente de NetScaler Gateway, configure las IP de intranet.
3. En el cuadro de diálogo **Vincular IP de intranet**, haga clic en **Acción** y, a continuación, en **Insertar**.
4. En Dirección IP y máscara de red, escriba la dirección IP y la máscara de subred y, a continuación, haga clic en **Agregar**.
5. Repita los pasos 3 y 4 para cada dirección IP que quiera agregar al grupo y, a continuación, haga clic en **Aceptar**.

Definir opciones de agrupación

Puede utilizar una directiva de sesión o la configuración global de NetScaler Gateway para controlar si se asignan direcciones IP de intranet durante una sesión de usuario. La definición de opciones de grupo de direcciones le permite asignar direcciones IP de intranet a NetScaler Gateway, al tiempo que inhabilita el uso de direcciones IP de intranet para un grupo determinado de usuarios.

Puede configurar grupos de direcciones mediante una directiva de sesión de una de las tres formas siguientes:

- `Nospillover` - Al configurar grupos de direcciones para direcciones IP de intranet, se obtiene una sesión con una IP disponible del grupo. Para los usuarios que han usado todas las direcciones IP de intranet disponibles, aparece la página Transferir inicio de sesión.
- **Spillover**: Cuando configura grupos de direcciones y la IP asignada se utiliza como dirección IP de intranet, la dirección IP asignada se utiliza para los usuarios que han utilizado todas las direcciones IP de intranet disponibles.
- **Desactivado** : los grupos de direcciones no están configurados.

> **Nota:**
>
> Si la dirección IP asignada no está configurada, se utiliza SNIP.

Para definir grupos de direcciones

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En Nombre , escriba un nombre para el perfil.
6. En la ficha **Configuración de red**, haga clic en **Avanzadas**.

7. Junto a IP de intranet, haga clic en **Sobrescribir global** y, a continuación, selecciona una opción.
8. Si selecciona **SPILLOVER** en el paso 9, junto a IP asignada, haga clic en **Supeditación global**, seleccione el nombre de host del dispositivo, haga clic en **Aceptar** y, a continuación, haga clic en **Crear**.
9. En el cuadro de diálogo **Crear directiva de sesión**, cree una expresión. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Configurar la página Transferir inicio de sesión

Si un usuario no tiene una dirección IP de intranet disponible y, a continuación, intenta establecer otra sesión con NetScaler Gateway, aparece la página Transferir inicio de sesión. La página Transferir inicio de sesión permite a los usuarios reemplazar su sesión actual de NetScaler Gateway por una nueva sesión.

La página Transferir inicio de sesión también se puede usar si se pierde la solicitud de cierre de sesión o si el usuario no realiza un cierre de sesión limpio. Por ejemplo:

- A un usuario se le asigna una dirección IP de intranet estática y ya tiene una sesión de NetScaler Gateway. Si el usuario intenta establecer una segunda sesión desde un dispositivo diferente, aparece la página Transferir inicio de sesión y el usuario puede transferir la sesión al nuevo dispositivo.
- A un usuario se le asignan cinco direcciones IP de intranet y tiene cinco sesiones a través de NetScaler Gateway. Si el usuario intenta establecer una sexta sesión, aparece la página Transferir inicio de sesión y el usuario puede optar por reemplazar una sesión existente por una nueva.

> **Notas:**
>
> - Si el usuario no tiene una dirección IP asignada disponible por la que no se puede establecer una nueva sesión, aparece un mensaje de error.
> - Citrix Secure Access para Android 23.12.1 y versiones posteriores admiten la función de transferencia de inicio de sesión de NetScaler Gateway en el modo Always On VPN.

La página Transferir inicio de sesión solo aparece si configura grupos de direcciones y inhabilita la transferencia.

Configurar un sufijo DNS

Cuando un usuario inicia sesión en NetScaler Gateway y se le asigna una dirección IP, se agrega un registro DNS para la combinación de nombre de usuario y dirección IP a la caché DNS de NetScaler Gateway. Puede configurar un sufijo DNS para que se agregue al nombre de usuario cuando se agregue el

registro DNS a la caché. Esto permite hacer referencia a los usuarios mediante el nombre DNS, que puede ser más fácil de recordar que una dirección IP. Cuando el usuario cierra sesión en NetScaler Gateway, el registro se elimina de la caché DNS.

Para configurar un sufijo DNS

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.
3. Junto a Solicitar perfil, haga clic en **Modificar**.
4. En la ficha **Configuración de red**, haga clic en **Avanzadas**.
5. Junto a Sufijo DNS de IP de intranet, haga clic en **Supeditación global**, escriba el sufijo DNS y, a continuación, haga clic en **Aceptar** tres veces.

Soporte para teléfonos VoIP

January 26, 2024

Al instalar NetScaler Gateway como un dispositivo independiente y los usuarios se conectan con el cliente Citrix Secure Access, NetScaler Gateway admite la comunicación bidireccional con teléfonos de voz sobre IP (VoIP).

NetScaler Gateway admite los siguientes softphones VoIP.

- Softphone de Cisco
- Softphone IP Avaya

Se admite la tunelización segura entre la centralita IP y el software softphone que se ejecuta en el dispositivo del usuario. Para permitir que el tráfico de VoIP atraviese el túnel seguro, debe instalar el cliente Citrix Secure Access y uno de los softphones compatibles en el mismo dispositivo de usuario. Cuando el tráfico VoIP se envía a través del túnel seguro, se admiten las siguientes funciones del softphone:

- Llamadas salientes que se realizan desde el softphone IP
- Llamadas entrantes que se colocan en el softphone IP
- Tráfico de voz bidireccional

La compatibilidad con softphones VoIP se configura mediante direcciones IP de intranet. Debe configurar una dirección IP de intranet para cada usuario. Si utiliza Cisco Softphone Communication,

después de configurar la dirección IP de la intranet y vincularla a un usuario, no se requiere ninguna configuración adicional. Para obtener más información sobre cómo configurar una dirección IP de intranet, consulte Configuración de grupos de direcciones.

Si habilita la tunelización dividida, cree una aplicación de intranet y especifique la aplicación Avaya Softphone. Además, debe habilitar la interceptación transparente.

Configurar interfaz de acceso

March 27, 2024

NetScaler Gateway incluye una página principal predeterminada que aparece después de que los usuarios inician sesión. La página principal predeterminada se denomina Interfaz de acceso. Utilice la interfaz de acceso como página principal o configure la interfaz web como página principal o como página principal personalizada.

La interfaz de acceso contiene tres paneles. Si tiene la interfaz web en la implementación, los usuarios pueden iniciar sesión en Receiver en el panel izquierdo de la interfaz de acceso. Si tiene StoreFront en la implementación, los usuarios no pueden iniciar sesión en Receiver desde el panel izquierdo.

La interfaz de acceso se utiliza para proporcionar enlaces a sitios web, tanto internos como externos, y enlaces a recursos compartidos de archivos en la red interna. Puede personalizar la interfaz de acceso de las siguientes formas:

- Cambiar la interfaz de acceso.
- Creación de vínculos de interfaz de acceso.

Los usuarios también pueden personalizar la interfaz de acceso agregando sus propios enlaces a sitios web y recursos compartidos de archivos. Los usuarios también pueden utilizar la página de inicio para transferir archivos de la red interna a su dispositivo.

> **Nota:**
>
> Cuando los usuarios inician sesión e intentan abrir recursos compartidos de archivos desde la interfaz de acceso, el recurso compartido de archivos no se abre y los usuarios reciben el mensaje de error "Error al establecer la conexión TCP con el servidor". Para resolver este problema, configure el firewall para permitir el tráfico desde la dirección IP del sistema NetScaler Gateway a la dirección IP del servidor de archivos en los puertos TCP 445 y 139.

Cambiar la interfaz de acceso

Es posible que quiera dirigir a los usuarios a una página principal personalizada, en lugar de depender de la interfaz de acceso. Para ello, instale la página principal en NetScaler Gateway y, a continuación,

configure la directiva de sesión para que utilice la nueva página principal.

Para instalar una página de inicio personalizada

1. En la utilidad de configuración, haga clic en la pestaña **Configuración** y, a continuación, en el panel de navegación, haga clic en **NetScaler Gateway .**
2. En el panel de detalles, en **Personalizar interfaz de acceso**, haga clic en **Cargar**la **interfaz de acceso.**
3. Para instalar la página principal desde un archivo de un equipo de la red, en Archivo local, haga clic en **Examinar**, vaya a el archivo y, a continuación, haga clic en **Seleccionar.**
4. Para utilizar una página principal instalada en NetScaler Gateway, en Ruta remota, haga clic en **Examinar**, seleccione el archivo y, a continuación, haga clic en **Seleccionar.**
5. Haga clic en **Cargar** y, a continuación, en **Cerrar.**

Reemplazar la interfaz de acceso por una página de inicio personalizada

Puede utilizar la configuración global o una directiva de sesión y un perfil para configurar una página principal personalizada que sustituya a la página principal predeterminada, la interfaz de acceso. Después de configurar la directiva, puede vincularla a un usuario, grupo, servidor virtual o de forma global. Al configurar una página principal personalizada, la interfaz de acceso no aparece cuando los usuarios inician sesión.

Configurar la página principal personalizada de forma global

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global.**
2. En el panel de detalles, en **Configuración** , haga clic en Cambiar la configuración global.
3. En la ficha **Experiencia del cliente**, en **Página**de inicio, haga clic en **Mostrar página de inicio y,** a continuación, introduzca la dirección web de la página principal personalizada.
4. Haga clic en **Aceptar** y luego en **Cerrar.**

Configurar una página principal personalizada en un perfil de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **Directivas de NetScaler Gateway** y, a continuación, haga clic en **Sesión.**
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar.**
3. En Nombre, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo.**
5. En **Nombre**, escriba un nombre para el perfil.

6. En la ficha **Experiencia del cliente**, junto a **Página**de inicio, haga clic en **Supedición global**, haga clic en **Mostrar página principal y,** a continuación, escriba la dirección web de la página principal.
7. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, seleccione Valor verdadero, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar.**

Crear y aplicar enlaces web

March 27, 2024

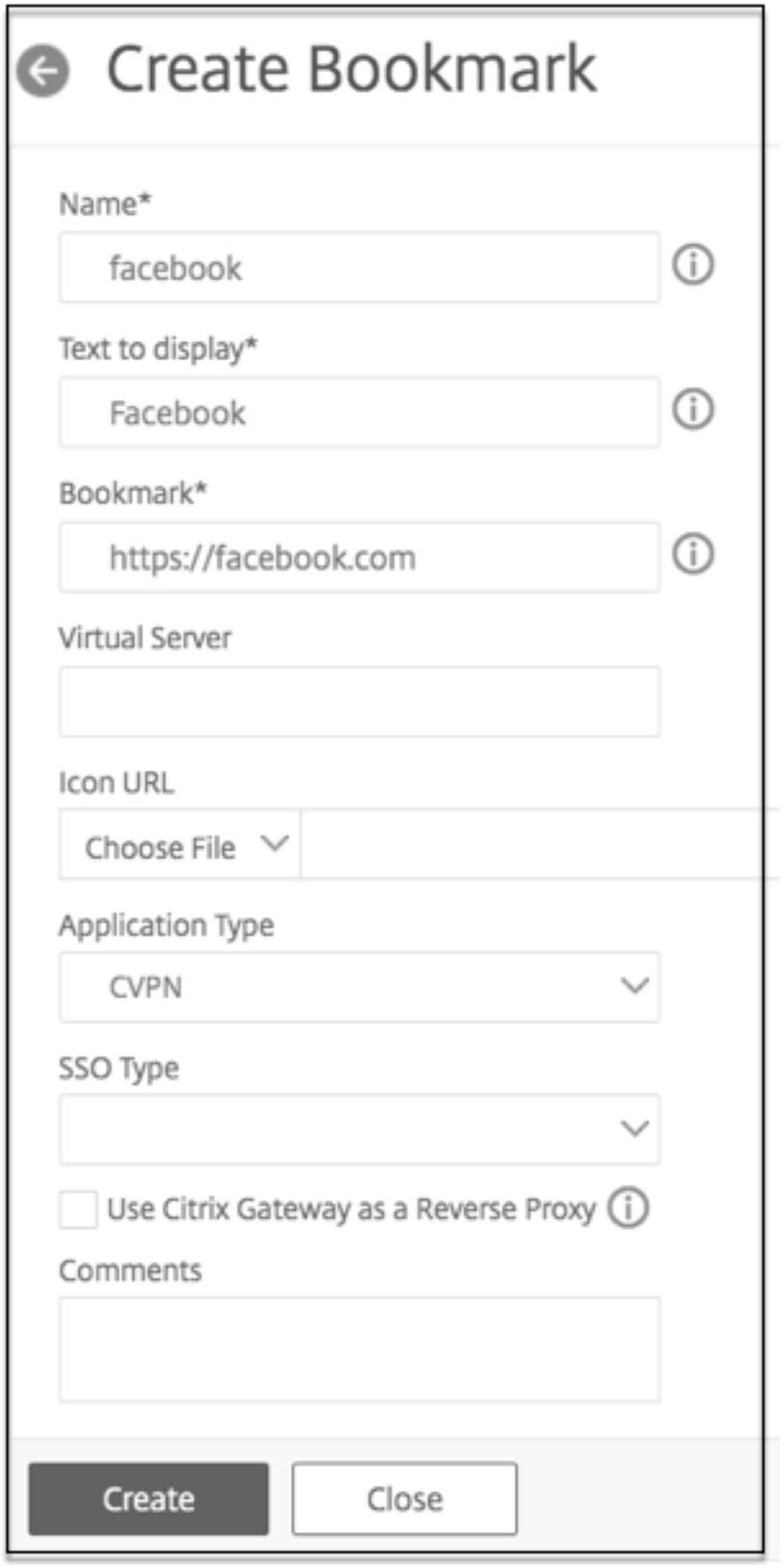
Puede configurar la interfaz de acceso para mostrar un conjunto de vínculos a los recursos internos disponibles para los usuarios. Para crear estos vínculos es necesario definir primero los vínculos como recursos. A continuación, los vincula a un usuario, grupo, servidor virtual o globalmente para activarlos en la interfaz de acceso. Los vínculos que cree aparecen en los paneles **Sitios web** de **Sitios web de empresa**.

> **Importante:**
>
> A partir de la versión 13.0 compilación 64.xx de NetScaler, los recursos compartidos de archivos a través de NetScaler Gateway no son compatibles.

Creación de marcadores de empresa

Para crear un vínculo de interfaz de acceso en una directiva de sesión

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Recursos** y, a continuación, haga clic en **Marcadores del portal.**
2. En el panel de detalles, haga clic en **Agregar.**



3. En **Nombre**, escriba un nombre para el marcador.

4. En **Texto para mostrar**, escriba la descripción del enlace. La descripción aparece en la **interfaz de acceso.**
5. En **Marcar como favorito**, escriba la dirección web de la aplicación.
6. En **Servidor virtual**, escriba el nombre del servidor virtual de equilibrio de carga/conmutación de contenido asociado. Este campo es opcional.
7. En **URL del icono**, los iconos cargados son compatibles con todos los temas, excepto el tema predeterminado. El tamaño máximo recomendado es de 70 x 70 píxeles. Le recomendamos que utilice imágenes transparentes. Este campo es opcional.
8. En **Tipo de aplicación**, seleccione el tipo de aplicación (VPN, VPN sin cliente o SaaS) que representa la URL. Este campo es opcional.
9. En **Tipo de SSO**, seleccione el tipo de SSO que quiera configurar para el marcador. Cuando se configura SSO, los usuarios pueden acceder a las aplicaciones sin tener que introducir sus credenciales en los inicios de sesión posteriores. Se admiten los siguientes tipos de SSO:

    - Puerta de enlace unificada: Esta configuración de SSO permite el acceso remoto seguro a varios recursos de una aplicación a través de una única URL.
    - Autenticación automática: En esta configuración de SSO, se pide a los usuarios de NetScaler Gateway que proporcionen las credenciales de inicio de sesión para acceder a la aplicación.
    - Autenticación basada en SAML: En esta configuración de SSO, NetScaler Gateway utiliza un IdP para validar los detalles del usuario, genera una afirmación de SAML y la envía al SP. Si se aprueba la validación, el SSO se ha realizado correctamente.

    > **Nota:**
    >
    > Si habilita el acceso sin cliente, puede asegurarse de que las solicitudes a los sitios web pasan por NetScaler Gateway. Por ejemplo, ha agregado un marcador para Google. Seleccione la casilla **Usar NetScaler Gateway como proxy inverso**. Al seleccionar esta casilla de verificación, las solicitudes del sitio web van del dispositivo del usuario a NetScaler Gateway y, a continuación, al sitio web. Al desactivar la casilla de verificación, las solicitudes van del dispositivo del usuario al sitio web. Esta casilla de verificación solo está disponible si habilita el acceso sin cliente.

10. Haga clic en **Crear** y, a continuación, en **Cerrar.**

Para enlazar un enlace de interfaz de acceso

Puede enlazar vínculos de la interfaz de acceso a las siguientes ubicaciones:

- Usuarios

- Grupos
- Servidores virtuales

Después de guardar la configuración, los vínculos están disponibles para los usuarios en la interfaz de acceso de la ficha **Inicio**, que es la primera página que ven los usuarios después de iniciar sesión correctamente.

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    - Amplíe **Administración de usuarios de NetScaler Gateway** y, a continuación, haga clic en **Usuarios AAA.**
    - Expanda **Administración de usuarios de NetScaler Gateway** y, a continuación, haga clic en **Grupos AAA.**
    - Amplíe **NetScaler Gateway** y, a continuación, haga clic en **Servidores virtuales.**
2. En el panel de detalles, realice una de las acciones siguientes:
    - Seleccione un usuario y, a continuación, haga clic en Abrir.
    - Seleccione un grupo y, a continuación, haga clic en Abrir.
    - Seleccione un servidor virtual y, a continuación, haga clic en Abrir.
3. En el cuadro de diálogo, haga clic en la ficha **Marcadores**.
4. En **Marcadores disponibles**, selecciona uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores en Marcadores configurados y, a continuación, en **Aceptar.**

Para enlazar marcadores de forma global mediante la interfaz gráfica de usuario

1. En la pestaña **Configuración** , en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en Configuración **global.**
2. En el panel de detalles, en **Marcadores**, haga clic en **Crear vínculos a las aplicaciones HTTP y de uso compartido de archivos de Windows a las que quiere que se pueda acceder en la página del portal de NetScaler Gateway**.

3. En el cuadro de diálogo **Configurar enlace global de VPN***, haga clic en **Agregar.**
4. En **Disponible**, seleccione uno o varios marcadores, haga clic en la flecha derecha para mover los marcadores en Configurado y, a continuación, en **Aceptar**.

Para agregar un marcador Enterprise mediante la CLI

En la línea de comandos, escriba:

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

Ejemplo:

Marcador web

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```

Para enlazar un marcador Enterprise mediante la CLI

Puede enlazar marcadores de empresa a usuario, grupo, servidor virtual y nivel global.

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  – urlName <string>
<!--NeedCopy-->
```

Ejemplo:

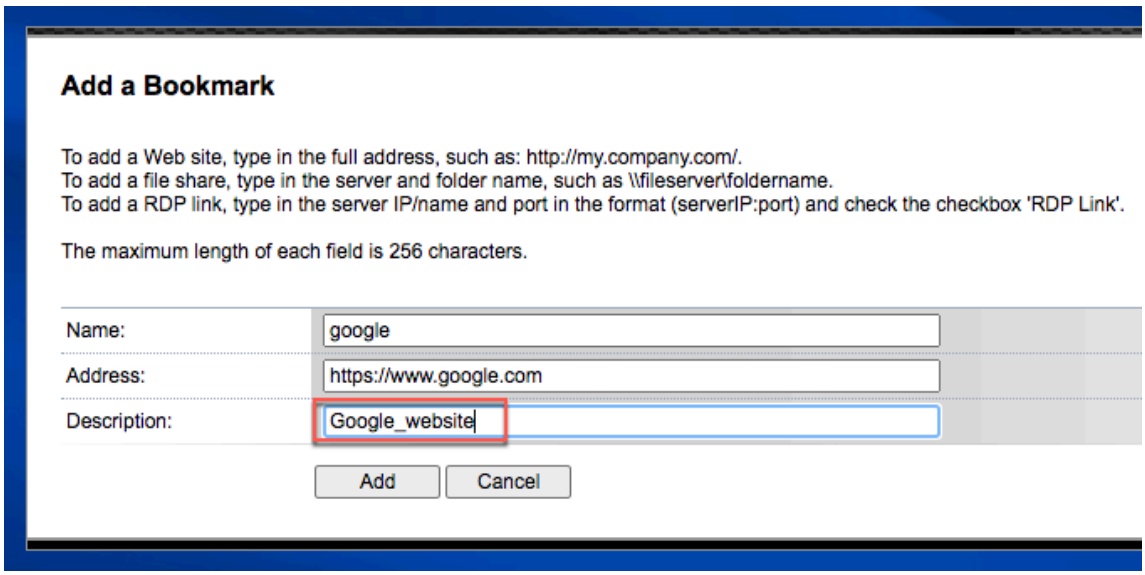

```
bind vpn global -urlName google
<!--NeedCopy-->
```

Creación de marcadores personales

Solo puede crear sitios web personales desde el servidor virtual VPN. No existe una interfaz gráfica de usuario de administración de NetScaler Gateway para agregar marcadores personales.

1. Inicie sesión en un servidor virtual VPN.
2. Haga clic en **Acceso a red** o **Acceso sin cliente** para agregar un marcador.
3. Haga clic en **Agregar**.

4. Introduzca los detalles del marcador, como el nombre del sitio web, la dirección y la descripción.



5. Haga clic en **Agregar**.

Los sitios web que ha agregado aparecen en las fichas respectivas.

Configurar tokens de nombre de usuario en marcadores

Puede configurar las URL de marcadores y recursos compartidos de archivos mediante un token especial,%username%. Cuando los usuarios inician sesión, el token se sustituye por el nombre de inicio de sesión de cada usuario. Por ejemplo, crea un marcador para un empleado llamado Jack para una carpeta como\\ EmployeeServer\%username%\. Cuando Jack inicia sesión, la URL del recurso compartido de archivos se asigna a\\ EmployeeServer\ Jack\. Al configurar tokens de nombre de usuario en los marcadores, tenga en cuenta las siguientes situaciones:

- Si utiliza un tipo de autenticación, el nombre de usuario sustituye al token%username%.

- Si utiliza la autenticación de dos factores, el nombre de usuario del tipo de autenticación principal se utiliza para reemplazar el token`username`%%.
- Si utiliza la autenticación de certificados de cliente, el campo de nombre de usuario del perfil de autenticación de certificados de cliente se utiliza para reemplazar el token`username`%%.

Directivas de tráfico

March 27, 2024

Las directivas de tráfico permiten configurar los siguientes ajustes para las conexiones de usuario:

- Aplicar tiempos de espera más cortos para aplicaciones sensibles a las que se accede desde redes que no son de confianza.
- Cambiar el tráfico de red para utilizar TCP en algunas aplicaciones. Si selecciona TCP, debe habilitar o inhabilitar el inicio de sesión único para determinadas aplicaciones.
- Identificar situaciones en las que desee utilizar otras funciones HTTP para el tráfico de clientes de Citrix Secure Access.
- Definición de las extensiones de nombre de archivo que se utilizan con la asociación de tipos de archivo.

Crear una directiva de tráfico

Para configurar una directiva de tráfico, crea un perfil y configura los siguientes parámetros:

- Protocolo (HTTP o TCP)
- Tiempo de espera de aplicación
- Inicio de sesión único en aplicaciones web
- Formulario de inicio de sesión único
- Asociación de tipos de archivos
- Plug-in repetidor
- Cuentas Kerberos Constrained Delegated (KCD)

Después de crear la directiva de tráfico, puede vincularla a servidores virtuales, usuarios, grupos o de forma global.

Por ejemplo, tiene la aplicación web PeopleSoft Human Resources instalada en un servidor de la red interna. Puede crear una directiva de tráfico para esta aplicación que defina la dirección IP de destino, el puerto de destino y puede establecer la cantidad de tiempo que un usuario puede permanecer conectado a la aplicación, por ejemplo, 15 minutos.

Si quiere configurar otras funciones, como la compresión HTTP en una aplicación, puede utilizar una directiva de tráfico para configurar la configuración. Al crear la directiva, utilice el parámetro HTTP para la acción. En la expresión, cree la dirección de destino del servidor que ejecuta la aplicación.

Ejemplos de expresiones de directivas de tráfico

Estos son ejemplos de expresiones de directivas de tráfico:

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\")|| HTTP.REQ.URL.CONTAINS(\"10.102.\")")"trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\")|| HTTP.REQ.URL.CONTAINS(\"homePage\"))"trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

Configurar una directiva de tráfico mediante la interfaz gráfica de usuario

1. Expanda **NetScaler Gateway > Directivas** y haga clic en **Tráfico**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear directiva de tráfico**, en **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En **Protocolo**, seleccione **HTTP** o **TCP**.

   Nota: Si selecciona TCP como protocolo, no podrá configurar el inicio de sesión único y la configuración se inhabilitará en el cuadro de diálogo del perfil.
7. En **AppTimeout (minutos)**, escriba el número de minutos. Esta configuración limita el tiempo que los usuarios pueden permanecer conectados a la aplicación web.
8. Para habilitar el inicio de sesión único en la aplicación web, en Inicio de **sesión único**, seleccione **ACTIVADO**.

   Nota : Si quieres usar el inicio de sesión único basado en formularios, puedes configurar los ajustes en el perfil de tráfico. Para obtener más información, consulte Configuración del inicio de sesión único basado en formularios.
9. Para especificar una asociación de tipos de archivo, en Asociación de **tipos de archivo**, seleccione **ACTIVADA**.

10. Para utilizar el complemento repetidor para optimizar el tráfico de red, en Citrix SD-WAN, seleccione **ACTIVADO**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.
11. Si configura KCD en el dispositivo, en Cuenta KCD, seleccione la cuenta.

    Para obtener más información sobre cómo configurar KCD en el dispositivo, consulte Configuración de la delegación restringida de Kerberos en un dispositivo NetScaler.
12. En el cuadro de diálogo Crear directiva de tráfico, cree o agregue una expresión, haga clic en **Crear y,** a continuación, en **Cerrar**.

Configurar el inicio de sesión único basado en formularios

El inicio de sesión único basado en formularios permite a los usuarios iniciar sesión una vez en todas las aplicaciones protegidas de la red. Al configurar el inicio de sesión único basado en formularios en NetScaler Gateway, los usuarios pueden acceder a aplicaciones web que requieren un inicio de sesión basado en formularios HTML sin tener que volver a escribir la contraseña. Sin el inicio de sesión único, los usuarios deben iniciar sesión por separado para acceder a cada aplicación.

Después de crear el perfil de inicio de sesión único del formulario, creará un perfil de tráfico y una directiva que incluya el perfil de inicio de sesión único del formulario. Para obtener más información, consulte Creación de una directiva de tráfico.

Configurar el inicio de sesión único basado en formularios

1. **Amplíe**NetScaler Gateway > Directivas y, a continuación,**haga clic en Tráfico.**
2. En el panel de detalles, haga clic en la ficha **Form SSO Profiles** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para el perfil.
4. En **URL de acción**, escriba la URL a la que se envía el formulario completado.

   Nota: La URL es la URL relativa raíz.
5. En **Nombre de usuario**, escriba el nombre del atributo del campo nombre de usuario.
6. En **Contraseña**, escriba el nombre del atributo del campo de contraseña.
7. En la **regla de éxito del SSO**, cree una expresión que describa la acción que realiza este perfil cuando lo invoca una directiva. También puede crear la expresión mediante los botones Prefijo, Agregar y Operador de este campo.

   Esta regla comprueba si Single Sign-On se ha realizado correctamente o no.

8. En **Pareja de valores de nombre**, escriba el valor del campo de nombre de usuario, seguido de una y comercial (&) y, a continuación, el valor del campo de contraseña.

   Los nombres de los valores están separados por una y comercial (&), como name1=value1&name2=value2.

9. En **Tamaño de respuesta**, escriba el número de bytes para permitir el tamaño de respuesta completo. Escriba el número de bytes de la respuesta que se analizará para extraer los formularios.
10. En **Extracción**, seleccione si el par nombre/valor es estático o dinámico. La configuración predeterminada es Dinámica.
11. En **Método de envío**, seleccione el método HTTP utilizado por el formulario de inicio de sesión único para enviar las credenciales de inicio de sesión al servidor de inicio de sesión. El valor predeterminado es Get.
12. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Configurar el inicio de sesión único de SAML

Puede crear un perfil SAML 1.1 o SAML 2.0 para el inicio de sesión único (SSO). Los usuarios pueden conectarse a aplicaciones web compatibles con el protocolo SAML para el inicio de sesión único. NetScaler Gateway admite el inicio de sesión único del proveedor de identidades (IdP) para aplicaciones web SAML.

Configurar el inicio de sesión único de SAML

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway\ > Directivas** y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, haga clic en la ficha Perfil de inicio de sesión único de SAML.
3. En el panel de detalles, haga clic en Agregar.
4. En Nombre , escriba un nombre para el perfil.
5. En Nombre del certificado de firma, introduzca el nombre del certificado X.509.
6. En ACS URL, introduzca el servicio de aserción de consumidor del proveedor de identidad o de servicio. AssertionConsumerServiceURL (URL ACS) proporciona capacidad de inicio de sesión único para los usuarios.
7. En Regla de estado de retransmisión, cree la expresión de la directiva a partir de expresiones de directiva guardadas y expresiones de uso frecuente. Seleccione en la lista Operador para definir cómo se evalúa la expresión. Para probar la expresión, haga clic en Evaluar.
8. En Enviar contraseña, selecciona ACTIVAR o DESACTIVAR.
9. En Nombre del emisor, introduzca la identidad de la aplicación SAML.
10. Haga clic en Crear y, a continuación, en Cerrar.

Vincular una directiva de tráfico

Puede enlazar directivas de tráfico a servidores virtuales, grupos, usuarios y a NetScaler Gateway Global. Puede utilizar la utilidad de configuración para enlazar una directiva de tráfico.

Enlazar una directiva de tráfico de forma global mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en Tráfico.
2. En el panel de detalles, seleccione una directiva y, a continuación, en Acción, haga clic en Enlaces globales.
3. En el cuadro de diálogo Vincular o desvincular directivas de tráfico, en Detalles, haga clic en Insertar directiva.
4. En Nombre de directiva, seleccione la directiva y, a continuación, haga clic en Aceptar.

Eliminar directivas de tráfico

Puede utilizar la utilidad de configuración para quitar las directivas de tráfico de NetScaler Gateway. Si utiliza la utilidad de configuración para quitar una directiva de tráfico y la directiva está vinculada al nivel de usuario, grupo o servidor virtual, primero debe desvincular la directiva. A continuación, puede quitar la directiva.

Desvincular una directiva de tráfico mediante la interfaz gráfica de usuario

1. Expanda **NetScaler Gateway y,** después, haga clic en **Servidores virtuales**
    - **Amplíe NetScaler Gateway > Administración**de usuarios y, a continuación, haga clic en **Grupos AAA**.
    - Expanda **NetScaler Gateway > Administración de usuarios** y haga clic en **Usuarios AAA**.
2. En el panel de detalles, seleccione un servidor virtual, un grupo o un usuario y, a continuación, haga clic en **Abrir**.
3. En el cuadro de diálogo **Configurar servidor virtual de NetScaler Gateway, Configurar grupo AAA** o **Configurar usuario AAA**, haga clic en la ficha **Directivas**.
4. Haga clic en **Tráfico**, seleccione la directiva y, a continuación, haga clic en **Desvincular directiva**.
5. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Una vez que la directiva de tráfico no esté vinculada, puede quitarla.

Eliminar una directiva de tráfico mediante la interfaz gráfica de usuario

1. Amplíe **NetScaler Gateway > Políticas** y, a continuación, haga clic en **Tráfico**.
2. En el panel de detalles, en la ficha Directivas, seleccione la directiva de tráfico y, a continuación, haga clic en **Quitar**.

Directivas de sesión

March 27, 2024

Una directiva de sesión es un conjunto de expresiones y configuraciones que se aplican a usuarios, grupos, servidores virtuales y de forma global.

Se utiliza una directiva de sesión para configurar la configuración de las conexiones de usuario. Puede definir los ajustes para configurar el software con el que los usuarios inician sesión, como el cliente Citrix Secure Access para Windows o el cliente Citrix Secure Access para Mac. También puede configurar los ajustes para exigir a los usuarios que inicien sesión con la aplicación Citrix Workspace o Secure Hub. Las directivas de sesión se evalúan y aplican después de autenticar al usuario.

Las directivas de sesión se aplican según las reglas siguientes:

- Las directivas de sesión siempre anulan la configuración global de la configuración.
- Los atributos o parámetros que no se establecen mediante una directiva de sesión se establecen en las directivas establecidas para el servidor virtual.
- Cualquier otro atributo que no esté establecido por una directiva de sesión o por el servidor virtual se establece en la configuración global.

> **Importante:**
>
> Las instrucciones siguientes son directrices generales para crear directivas de sesión. Existen instrucciones específicas para configurar directivas de sesión para distintas configuraciones, como el acceso sin cliente o el acceso a aplicaciones publicadas. Las instrucciones pueden contener instrucciones para configurar un ajuste específico. Sin embargo, esta configuración puede ser una de las muchas que se incluyen en un perfil y una directiva de sesión. Las instrucciones le indican que cree una configuración dentro de un perfil de sesión y, a continuación, aplique el perfil a una directiva de sesión. Puede cambiar la configuración de un perfil y una directiva sin crear una directiva de sesión. Además, puede crear toda la configuración a nivel global y, a continuación, crear una directiva de sesión para anular la configuración global.

Si implementa Citrix Endpoint Management o StoreFront en su red, Citrix recomienda utilizar el Asistente de configuración rápida para configurar perfiles y directivas de sesión. Al ejecutar el asistente,

define la configuración de su implementación. A continuación, NetScaler Gateway crea las directivas de autenticación, sesión y acceso sin cliente necesarias.

Crear una directiva de sesión

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda NetScaler Gateway > Políticas y, a continuación, haga clic en Sesión.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Solicitar perfil, haz clic en Nuevo .
5. En Nombre , escriba un nombre para el perfil.
6. Complete la configuración del perfil de sesión y, a continuación, haga clic en Crear.
7. En el cuadro de diálogo Crear perfil de sesión, agregue una expresión para la directiva, haga clic en Crear y, a continuación, haga clic en Cerrar.
   Nota: En la expresión, seleccione Valor
   verdadero para que la directiva se aplique siempre al nivel al que está vinculada.

Ejemplos de expresiones de directivas de sesión

A continuación se muestran los ejemplos de expresiones de las directivas de sesión:

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")|| HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")"sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT"sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

Enlazar directivas de sesión

Después de crear una directiva de sesión, enlaza a un usuario, grupo, servidor virtual o globalmente. Las directivas de sesión se aplican como jerarquía en el siguiente orden:

- Usuarios
- Grupos
- Servidores virtuales
- Globalmente

Enlazar una directiva de sesión a un servidor virtual mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. Seleccione un servidor virtual y haga clic en **Modificar**. También puede crear un nuevo servidor virtual.
3. Desplácese hacia abajo hasta la sección **Directivas** y haga clic en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión**.
5. En **Elegir tipo**, seleccione **Solicitud**y haga clic en **Continuar**.
6. En **Seleccionar directiva**, seleccione la directiva que quiere enlazar a este servidor virtual.
7. En **Prioridad**, introduzca el número de prioridad de la directiva.
8. Haga clic en **Bind**.

Enlazar una directiva de sesión a un grupo de autenticación, autorización y auditoría mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Administración de usuarios > Grupos AAA**.
2. Seleccione un grupo de autenticación, autorización y auditoría existente y haga clic en **Modificar**. También puede crear un grupo de autenticación, autorización y auditoría.
3. En **Configuración avanzada**, haga clic en **Directivas y,** a continuación, en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión**y haga clic en **Continuar**.
5. En **Seleccionar directiva**, seleccione la directiva que desea vincular a este grupo de autenticación, autorización y auditoría.
6. En **Prioridad**, introduzca el número de prioridad de la directiva.
7. Haga clic en **Bind**.

Enlazar una directiva de sesión a un usuario de autenticación, autorización y auditoría mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Administración de usuarios > Usuarios AAA**.
2. Seleccione un usuario de NetScaler existente y haga clic en **Modificar**. También puede crear un usuario de autenticación, autorización y auditoría.
3. En **Configuración avanzada**, haga clic en **Directivas y,** a continuación, en el icono **+**.
4. En **Elegir directiva**, seleccione **Sesión**y haga clic en **Continuar**.
5. En **Seleccionar directiva**, seleccione la directiva que desea vincular a este usuario de autenticación, autorización y auditoría.
6. En **Prioridad**, introduzca el número de prioridad de la directiva.
7. Haga clic en **Bind**.

Nota: Para obtener más información sobre la prioridad, consulte https://support.citrix.com/article/CTX214588.

Crear un perfil de sesión

Un perfil de sesión contiene la configuración de las conexiones de usuario.

Los perfiles de sesión especifican las acciones que se aplican a una sesión de usuario si el dispositivo de usuario cumple las condiciones de expresión de la directiva. Los perfiles se utilizan con directivas de sesión. Puede utilizar la utilidad de configuración para crear perfiles de sesión por separado de una directiva de sesión y, a continuación, utilizarlo para varias directivas. Solo puede utilizar un perfil con una directiva.

Configurar los ajustes de red para las conexiones de usuario en un perfil de sesión

Puede usar la ficha **Configuración de red** del perfil de sesión para configurar los siguientes ajustes de red para las conexiones de usuario:

- Servidor DNS
- Dirección IP del servidor WINS
- Dirección IP asignada que puede utilizar como dirección IP de intranet
- Configuración de desbordamiento para grupos de direcciones (direcciones IP de intranet)
- Sufijo DNS IP de intranet
- Puertos HTTP
- Configuración de tiempo de espera forzado

Configurar los ajustes de conexión en un perfil de sesión

Puede usar la ficha **Experiencia del cliente** del perfil de sesión para configurar los siguientes ajustes de conexión:

- Interfaz de acceso o página de inicio personalizada
- Dirección web para correo electrónico basado en web, como Outlook Web Access
- tipo de complemento (cliente Citrix Secure Access para Windows o cliente Citrix Secure Access para macOS X)
- Túneles divididos
- Configuración de tiempo de espera de sesión e inactividad
- Acceso sin cliente
- Codificación URL de acceso sin cliente
- tipo de complemento (Windows o Mac)
- Inicio de sesión único en aplicaciones web
- Índice de credenciales para autenticación
- Inicio de sesión único con Windows
- Comportamiento de limpieza de clientes

- Scripts de inicio de sesión
- Configuración de depuración del cliente
- DNS dividido
- Acceso a direcciones IP de redes privadas y acceso LAN local
- Opciones del cliente
- Configuración de proxy

Para obtener más información sobre la configuración de las conexiones de usuario, consulte Configuración de conexiones para el cliente Citrix Secure Access.

Configurar los ajustes de seguridad en un perfil de sesión

Puede usar la ficha **Seguridad de** un perfil de sesión para configurar los siguientes ajustes de seguridad:

- Acción de autorización predeterminada (permitir o denegar)
- Secure Browse para conexiones desde dispositivos iOS
- Grupos de cuarentena
- Grupos de autorización

Para obtener más información sobre cómo configurar la autorización en NetScaler Gateway, consulte Configuración de la autorización.

Configurar los ajustes de Citrix Virtual Apps and Desktops en un perfil de sesión

Puede usar la ficha **Aplicaciones publicadas** de un perfil de sesión para configurar los siguientes parámetros para las conexiones a los servidores que ejecutan Citrix Virtual Apps and Desktops:

- ICA Proxy, es decir, conexiones de clientes mediante la aplicación Citrix Workspace
- Dirección de Interfaz Web
- Modo portal de Interfaz Web
- Inicio de sesión único en el dominio de la comunidad de servidores
- Página principal de la aplicación Citrix Workspace
- Dirección de servicios de cuenta

Para obtener más información sobre cómo configurar los valores para conectarse a aplicaciones publicadas en un conjunto de servidores, consulte Proporcionar acceso a aplicaciones publicadas y escritorios virtuales a través de la Interfaz Web.

Puede crear perfiles de sesión independientemente de una directiva de sesión. Al crear la directiva, puede seleccionar el perfil que quiere asociar a la directiva.

Para crear un perfil de sesión mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Políticas y, a continuación,** haga clic en **Sesión**.
2. En el panel de detalles, haga clic en la ficha **Perfiles** y, a continuación, haga clic en **Agregar**.
3. Configure los ajustes del perfil, haga clic en **Crear y,** a continuación, en **Cerrar** .

Después de crear un perfil, puede incluirlo en una directiva de sesión.

Para agregar un perfil a una directiva de sesión mediante la interfaz gráfica de usuario

1. En la utilidad de configuración, en el panel de navegación, expanda **Access Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En la ficha **Directivas**, realice una de las siguientes acciones:
   - Haga clic en **Agregar** para crear una directiva de sesión.
   - Seleccione una directiva y, a continuación, haga clic en **Abrir**.
3. En **Solicitar perfil**, seleccione un perfil de la lista.
4. Termine de configurar la directiva de sesión y, a continuación, realice una de las siguientes acciones:
   a) Haga clic en **Crear y,** a continuación, en **Cerrar** para crear la directiva.
   b) Haga clic en **Aceptar y,** a continuación, en **Cerrar** para modificar la directiva.

Función de directivas avanzadas para marcadores empresariales

March 27, 2024

Los marcadores empresariales (URL de VPN) se pueden configurar como directivas avanzadas.

> **Notas:**
>
> - NetScaler Gateway admite los protocolos HTTP, HTTPs y RDP para los marcadores empresariales.
> - NetScaler Gateway solo admite URL absolutas para los marcadores empresariales.

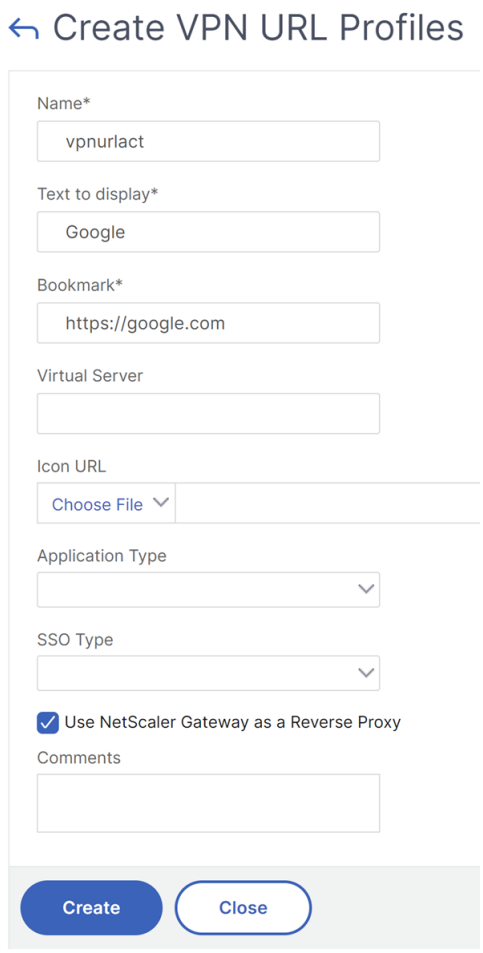
Configurar URL de VPN como directiva avanzada

En la GUI

1. Cree un perfil URL de VPN.

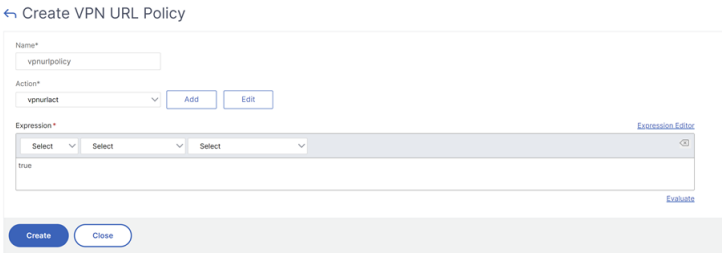
- Vaya a **Configuración > NetScaler Gateway > Directivas > URL de VPN**.
- En la página **Directivas y perfiles de URL de VPN**, seleccione la ficha **Perfiles de URL de VPN** y haga clic en **Agregar**.
- Actualice los campos obligatorios y haga clic en **Crear**.
  - Nombre: nombre para el perfil URL de la VPN.
  - Texto que se va a mostrar: una breve descripción del enlace. La descripción aparece en la interfaz de acceso.
  - Marcador: dirección web de la aplicación.
  - Servidor virtual: nombre del servidor virtual de equilibrio de carga o conmutación de contenido asociado que está configurado. Este campo es opcional.
  - URL del icono: los iconos cargados en este campo son compatibles con todos los temas, excepto el tema predeterminado. El tamaño máximo recomendado es de 70 x 70 píxeles. Le recomendamos que utilice imágenes transparentes. Este campo es opcional.
  - Tipo de aplicación: seleccione el tipo de aplicación (VPN, VPN sin cliente o SaaS) que representa la URL. Este campo es opcional.
  - Tipo de SSO: tipo de SSO que quieres configurar para el marcador. Cuando se configura SSO, los usuarios pueden acceder a las aplicaciones sin tener que introducir sus credenciales en los inicios de sesión posteriores. Se admiten los siguientes tipos de SSO:
    * Puerta de enlace unificada: Esta configuración de SSO permite el acceso remoto seguro a varios recursos de una aplicación a través de una única URL.
    * Autenticación automática: En esta configuración de SSO, se pide a los usuarios de NetScaler Gateway que proporcionen las credenciales de inicio de sesión para acceder a la aplicación.
    * Autenticación basada en SAML: En esta configuración de SSO, NetScaler Gateway utiliza un IdP para validar los detalles del usuario, genera una afirmación de SAML y la envía al SP. Si se aprueba la validación, el SSO se ha realizado correctamente.

> **Note:**
>
> If you enable clientless access, you can make sure that requests to websites go through NetScaler Gateway. For example, you added a bookmark for Google. Select the Use NetScaler Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to NetScaler Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.



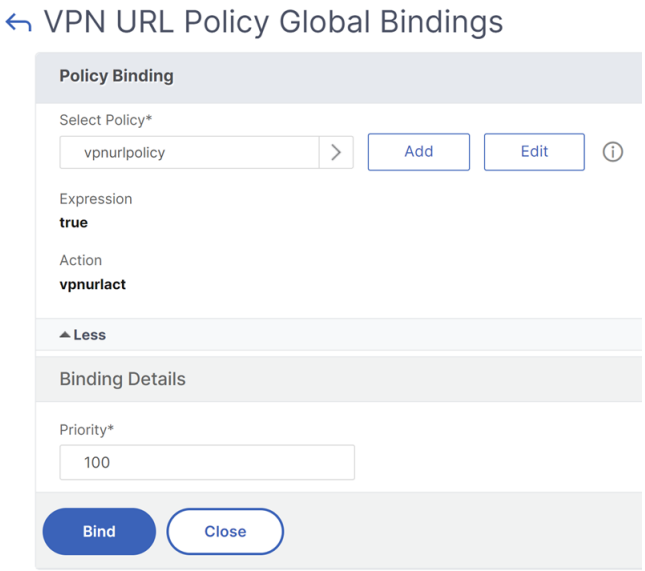
2. Cree una directiva de URL de VPN.

   - Vaya a **Configuración > NetScaler Gateway > Directivas > URL de VPN**.
   - En la página **Directivas y perfiles de URL de VPN**, seleccione la ficha **Directiva de URL de VPN** y haga clic en **Agregar**.
   - Actualice los campos obligatorios y haga clic en **Crear**.
     - Nombre: nombre para la directiva de URL de VPN.
     - Acción: Seleccione el perfil URL de VPN configurado. Si no hay ningún perfil en la lista desplegable, haga clic en Agregar y repita el paso 1.
     - Expresión: consulte Directivas y expresiones para obtener información sobre las expresiones de directiva avanzadas.



3. Enlazar la directiva de URL de VPN a un punto de enlace.

   - Vaya a **Configuración > NetScaler Gateway > Directivas > URL de VPN**.
   - En la página **Directivas y perfiles de URL de VPN**, seleccione la ficha **Directiva de URL de VPN** .
   - Seleccione **Enlaces globales** en la lista desplegable **Seleccionar acción** .
   - Seleccione la directiva de URL de VPN. Si no aparece ninguna directiva, haga clic en **Agregar** y repita el paso 2.
   - En la sección **Detalles de enlace**, asigne una prioridad a la directiva de URL de VPN.



En la CLI

Cree una acción de URL de VPN:

En el símbolo del sistema, escriba lo siguiente:

```
add vpn urlAction <name> -linkName <string> -actualURL <string> \[-
    vServerName <string>] \[-clientlessAccess \( ON | OFF )] \[-comment
    <string>] \[-iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype
     <applicationtype>] \[-samlSSOProfile <string>]
```


NetScaler Gateway admite las siguientes operaciones para la acción de URL de VPN:

- **add**

```
add vpn urlAction <name> -linkName <string> -actualURL <string>
   \[-vServerName <string>] \[-clientlessAccess \( ON | OFF )]
   \[-comment <string>] \[-iconURL <URL>] \[-ssotype <ssotype>]
   \[-applicationtype <applicationtype>] \[-samlSSOProfile <
   string>]
```

- **set**

```
set vpn urlAction <name> \[-vServerName <string>] \[-
   clientlessAccess \( ON | OFF )] \[-comment <string>] \[-
   iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype <
   applicationtype>] \[-samlSSOProfile <string>]
```

- **unset**

```
unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
   comment] [-iconURL] [-ssotype] [-applicationtype] [-
   samlSSOProfile]
```

> **Nota:**
>
> Si configura el acceso sin cliente en ON, puede asegurarse de que las solicitudes a los sitios web vayan del dispositivo del usuario a NetScaler Gateway y, después, al sitio web.

- **show**

```
show vpn urlAction [<name>]
```

- **remove**

```
remove vpn urlAction <name>
```

- **rename**

```
rename vpn urlAction <name>@ <newName>@
```

Cree una directiva de URL de VPN:

NetScaler Gateway admite las siguientes operaciones para la directiva de URL de VPN:

- **add**

```
add vpn urlPolicy <name> -rule <expression> -action <string> [-
   comment <string>] [-logAction <string>]
```

- **set**


```
set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
    [-comment <string>] [-logAction <string>]
```

- **unset**

```
unset vpn urlPolicy <name> [-comment] [-logAction]
```

- **show**

```
show vpn urlPolicy [<name>]
```

- **remove**

```
remove vpn urlPolicy <name>
```

- **rename**

```
rename vpn urlpolicy <name>@ <newName>@
```

- **stat**

```
stat vpn urlpolicy \[<name>] \[-detail] \[-fullValues] \[-ntimes
    <positive\_integer>] \[-logFile <input\_filename>] \[-
    clearstats \( basic | full )]
```

Enlazar la directiva a un punto de enlace:

NetScaler Gateway admite las siguientes operaciones para vincular directivas de URL de VPN:

- **bind**

```
bind vpn vserver <vserver name> -policy <string> -priority <
    positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
     [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
bind aaa group <groupName> -policy <string> [-priority <
    positive_integer>] [-type <type>] [-gotoPriorityExpression <
    expression>]
```

- **unbind**

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```


> **Nota:**
>
> Los puntos de enlace son `aaauseraaagroup`, `vpnvserver`, y `vpnglobal`.

Directivas de dispositivos de punto final

March 27, 2024

Endpoint Analysis (EPA) es un proceso que escanea el dispositivo de un usuario y detecta información, como la presencia y el nivel de versión de las actualizaciones del sistema operativo, el antivirus, el firewall y el software del explorador web. Endpoint Analysis le permite determinar si el dispositivo de un usuario cumple con sus requisitos antes de conectarse a la red. También se puede configurar para comprobar periódicamente si hay cambios mientras el usuario permanece conectado. Puede comprobar los archivos, los procesos y las entradas de registro en el dispositivo del usuario durante la sesión del usuario para asegurarse de que el dispositivo sigue cumpliendo con los requisitos.

> **Importante:**
>
> - El objetivo de Endpoint Analysis es analizar el dispositivo del usuario en función de criterios de cumplimiento predeterminados y no aplica ni valida la seguridad de los dispositivos de los usuarios finales. Se recomienda utilizar sistemas de seguridad de dispositivos de punto final para proteger los dispositivos de los ataques de los administradores locales.
> - El cliente EPA está disponible como cliente independiente y también se incluye junto con el cliente Citrix Secure Access. El cliente de Citrix EPA y el cliente de Citrix Secure Access son independientes.

Cómo funcionan las directivas de endpoint

Puede configurar NetScaler Gateway para comprobar si un dispositivo de usuario cumple ciertos requisitos antes de que el usuario inicie sesión. Esto se denomina directiva de preautenticación. Puede configurar NetScaler Gateway para que compruebe si un dispositivo de usuario tiene antivirus, firewall, antispam, procesos, archivos, entradas de registro, seguridad de Internet o sistemas operativos que especifique en la directiva. Si el dispositivo de usuario no supera el análisis previo a la autenticación, los usuarios no pueden iniciar sesión.

Para comprobar otros requisitos que no se utilizan en una directiva de preautenticación, puede configurar una directiva de sesión y vincularla a un usuario o grupo. Este tipo de directiva se denomina directiva de posautenticación y se ejecuta durante la sesión del usuario para garantizar que los criterios requeridos, como el software antivirus o un proceso, sigan siendo compatibles.

Al configurar una directiva de preautenticación o posautenticación, NetScaler Gateway descarga el plug-in de Endpoint Analysis y, a continuación, realiza el escaneo en el dispositivo de los usuarios. Cada vez que un usuario inicia sesión, el complemento Endpoint Analysis se ejecuta automáticamente.

Puede usar los tres tipos de directivas siguientes para configurar las directivas de dispositivos de punto final:

- Directiva de preautenticación que utiliza un parámetro Sí o No. El análisis determina si el dispositivo del usuario cumple los requisitos especificados. Si se produce un error en el análisis, el usuario no puede introducir las credenciales en la página de inicio de sesión.
- Directiva de sesión condicional y que se puede utilizar para SmartAccess.
- Expresión de verificación del dispositivo cliente dentro de una directiva de sesión. Si el dispositivo de usuario no cumple con los requisitos de la expresión de verificación del dispositivo cliente, puede configurar los usuarios para que se coloquen en un grupo de cuarentena. Si el dispositivo del usuario supera el análisis, los usuarios se pueden colocar en un grupo diferente que podría requerir otras comprobaciones.

Puede incorporar la información detectada en las directivas, lo que le permite conceder diferentes niveles de acceso según el dispositivo del usuario. Por ejemplo, puede proporcionar acceso completo con permiso de descarga a los usuarios que se conectan de forma remota desde dispositivos de usuario que tienen requisitos actuales de software antivirus y firewall. Para los usuarios que se conecten desde dispositivos no compatibles, puede proporcionar un nivel de acceso más restringido que permita a los usuarios modificar documentos en servidores remotos sin descargarlos. Todos los dispositivos que ejecutan EPA se consideran dispositivos no conformes.

Endpoint Analysis realiza los siguientes pasos básicos:

- Examina un conjunto inicial de información sobre el dispositivo del usuario para determinar qué análisis se deben aplicar.
- Ejecuta todos los escaneos aplicables. Cuando los usuarios intentan conectarse, el plug-in de Endpoint Analysis comprueba en el dispositivo del usuario los requisitos especificados en la directiva de sesión o de preautenticación. Si el dispositivo del usuario supera el análisis, los usuarios pueden iniciar sesión. Si el dispositivo del usuario no supera el análisis, los usuarios no pueden iniciar sesión.

  Nota: Los escaneos de Endpoint Analysis finalizan antes de que la sesión del usuario utilice una licencia.
- Compara los valores de las propiedades detectados en el dispositivo del usuario con los valores de propiedad deseados que figuran en los escaneos configurados.
- Produce un resultado que verifica si se han encontrado los valores de propiedad deseados.

> **Atención:**
>
> Las instrucciones para crear directivas de Endpoint Analysis son directrices generales. Puede tener muchas opciones de configuración dentro de una directiva de sesión. Las instrucciones específicas para configurar directivas de sesión pueden contener instrucciones para configurar una configuración específica. Sin embargo, esta configuración puede ser una de las muchas que se incluyen en un perfil y una directiva de sesión.

Ejemplos de expresiones de EPA

A continuación se muestran los ejemplos de expresión de algunos componentes de EPA, como el proceso de eliminación, la eliminación de archivos y el certificado de dispositivo:

- Windows:
  - Proceso de eliminación: `sys.client_expr(\“proc_0_perl\“)-killProcess processToKill.exe`
  - Certificado de dispositivo:`sys.client_expr(“device-cert_0_0”)`
  - Eliminar archivos:`sys.client_expr(\“proc_0_perl\“)-deletefiles “C:/removefile.txt”`
- MAC
  - Proceso de eliminación: `sys.client_expr(\“proc_0_perl\“)-killProcess processToKill.exe`
  - Certificado de dispositivo:`sys.client_expr(“device-cert_0_0”)`
  - Eliminar archivos:`sys.client_expr(\“proc_0_perl\“)-deletefiles “C:/removefile.txt”`

Evaluar opciones de inicio de sesión de usuario

Cuando los usuarios inician sesión, pueden optar por omitir el análisis de Endpoint Analysis. Si los usuarios omiten el análisis, NetScaler Gateway procesa esta acción como un análisis de punto final erróneo. Cuando los usuarios no realizan el escaneo, solo tienen acceso a la interfaz web o mediante el acceso sin cliente.

Por ejemplo, desea proporcionar acceso a los usuarios mediante el cliente Citrix Secure Access. Para iniciar sesión en NetScaler Gateway con el complemento, los usuarios deben estar ejecutando una aplicación antivirus, como Norton Antivirus. Si el dispositivo de usuario no ejecuta la aplicación, los usuarios solo pueden iniciar sesión con Receiver y utilizar aplicaciones publicadas. También puede configurar el acceso sin cliente, que restringe el acceso a aplicaciones específicas, como Outlook Web Access.

Para configurar NetScaler Gateway para lograr este caso de inicio de sesión, asigne una directiva de sesión restrictiva como directiva predeterminada. A continuación, configure la configuración para actualizar a los usuarios a una directiva de sesión privilegiada cuando el dispositivo de usuario supera el análisis de Endpoint Analysis. En ese momento, los usuarios tienen acceso a la capa de red y pueden iniciar sesión con el cliente Citrix Secure Access.

Para configurar NetScaler Gateway para que aplique primero la directiva de sesión restrictiva, lleve a cabo los siguientes pasos:

- Configure la configuración global con el proxy ICA habilitado y todos los demás ajustes necesarios si la aplicación especificada no se está ejecutando en el dispositivo del usuario.
- Cree una directiva de sesión y un perfil que habiliten el cliente Citrix Secure Access.
- Cree una expresión dentro de la parte de reglas de la directiva de sesión para especificar la aplicación, como `(client.application.process(symantec.exe)exists)`

  Cuando los usuarios inician sesión, la directiva de sesión se aplica primero. Si Endpoint Analysis falla o el usuario omite el análisis, NetScaler Gateway ignora la configuración de la directiva de sesión (la expresión de la directiva de sesión se considera falsa). Como resultado, los usuarios tienen acceso restringido mediante la Interfaz Web o el acceso sin cliente. Si se aprueba Endpoint Analysis, NetScaler Gateway aplica la directiva de sesión y los usuarios tienen acceso total al cliente Citrix Secure Access.

Omitir el escaneo de EPA

Puede omitir el análisis de EPA solo para la posautenticación y la autenticación avanzada. Skip EPA está disponible en los exploradores de todos los sistemas operativos compatibles. Los usuarios deben hacer clic en el botón **Omitir EPA** que aparece al acceder a la puerta de enlace. Si los usuarios omiten el análisis, NetScaler Gateway procesa esta acción como un análisis de punto final erróneo. Cuando los usuarios no realizan el escaneo, solo tienen acceso a la interfaz web o mediante el acceso sin cliente.

Consulte también https://support.citrix.com/article/CTX200748.

Análisis de endpoint Analysis compatibles con Ubuntu

Los siguientes análisis de Endpoint Analysis (EPA) son compatibles con el complemento EPA instalado para el sistema operativo Ubuntu. Se muestra una expresión de ejemplo para configurar cada uno de los escaneos junto con los escaneos de la EPA. Puede configurar estas expresiones en las directivas de autenticación.

- **Archivo**

  - **Existencia**: sys.client_expr("file_0_/home/user/test.txt")
  - **Suma de comprobación MD5**: sys.client_expr("file_0*/home/user/test.txt_md5* ce780e271debcc29f551
)
  - **Texto dentro de un archivo (permite expresiones regulares)**: sys.client_expr("file_0_/home/user/test.txt_search_cloud")

- **Process**
  - **Existencia**: sys.client_expr("proc_0_perl")
  - **Suma de comprobación MD5**: sys.client_expr("proc_0*perl_md5* c060d3a5f97e27066cef8c116785567a
)
  - **Ruta**: sys.client_expr("proc_0*perl_path*/usr/bin/perl")

- **Dispositivo del sistema de archivos o Nombre del punto de montaje**: sys.client_expr("mountpoint_0_/sys")

Si utiliza directivas avanzadas, las expresiones de cada análisis se pueden generar desde la GUI (**Seguridad > AAA > Directivas > Autenticación > Directivas avanzadas > EPA**).

Nota: En la página Editor de expresiones, para el cliente Linux, puede seleccionar **Común** y, a continuación, seleccionar **Proceso, Archivo** o **Punto de montaje**.

Directivas y perfiles de preautenticación

March 27, 2024

> **Importante:**
>
> El objetivo de Endpoint Analysis es analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no hace cumplir ni validar la seguridad de los dispositivos de los usuarios finales. Se recomienda utilizar sistemas de seguridad de dispositivos de punto final para proteger los dispositivos de los ataques de los administradores locales.

Puede configurar NetScaler Gateway para comprobar los dispositivos de un usuario antes de que se autentiquen en NetScaler Gateway. Esto se puede usar para restringir el acceso si el dispositivo del usuario no cumple con los requisitos de la organización. Las comprobaciones de dispositivos se pueden implementar mediante directivas individuales específicas de un servidor virtual o de forma global, tal como se describe en los dos procedimientos siguientes.

Las directivas de preautenticación consisten en un perfil y una expresión. El perfil se configura para que utilice una expresión que permita o deniegue la ejecución de un proceso en el dispositivo del usuario. Por ejemplo, el archivo de texto clienttext.txt se ejecuta en el dispositivo del usuario. Cuando

el usuario inicia sesión en NetScaler Gateway, puede permitir o denegar el acceso en función de si el archivo de texto se está ejecutando. Si no quiere permitir que los usuarios inicien sesión cuando se ejecuta el proceso, puede configurar un perfil de preautenticación para detener el proceso antes de que los usuarios inicien sesión.

Puede configurar los siguientes ajustes para las directivas de preautenticación:

- Expresión. Incluye la siguiente configuración para ayudarle a crear expresiones:
  - Expresión. Muestra todas las expresiones.
  - Haga coincidir cualquier expresión. Configura la directiva para que coincida con cualquiera de las expresiones presentes en la lista de expresiones seleccionadas.
  - Coincidir con todas las expresiones. Configura la directiva para que coincida con todas las expresiones presentes en la lista de expresiones seleccionadas.
  - Expresiones tabulares. Crea una expresión compuesta con las expresiones existentes mediante los operadores `OR (||)` `or AND (&&)`.
  - Formato libre avanzado. Crea expresiones compuestas personalizadas mediante los nombres de las expresiones y los operadores `OR (||)` `and AND (&&)`. Elija solo las expresiones que necesite y omita otras expresiones de la lista de expresiones seleccionadas.
  - Add: Crea una expresión.
  - Modificar. Modifica una expresión existente.
  - Remove: Elimina la expresión seleccionada de la lista de expresiones compuestas.
  - Expresiones con nombre. Seleccione una expresión con nombre configurada. Puede seleccionar expresiones con nombre en el menú de expresiones ya presentes en NetScaler Gateway.
  - Agregar expresión. Agrega la expresión con nombre seleccionada a la directiva.
  - Reemplazar expresión. Reemplaza la expresión con nombre seleccionada en la directiva.
  - Vista previa de expresión. Muestra la cadena detallada que se configura en NetScaler Gateway al seleccionar una expresión con nombre.

Configurar el perfil de preautenticación

Para configurar un perfil de preautenticación de forma global mediante la interfaz gráfica de usuario

1. En la ficha Configuración, haga clic en **NetScaler Gateway** y, a continuación, en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración de preautenticación**.
3. En el cuadro de diálogo **Configuración de preautenticación global**, configure la configuración:
   a) En **Acción** , selecciona **Permitir o Denegar** .

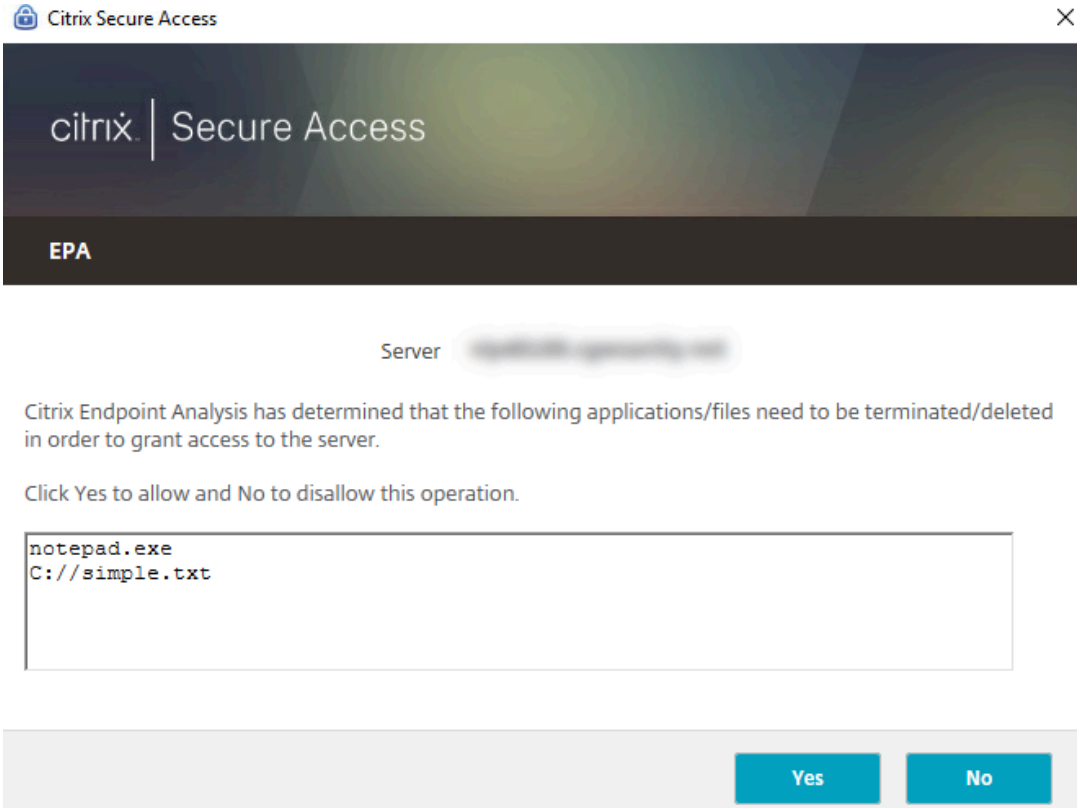
Deniega o permite que los usuarios inicien sesión después de que se produzca Endpoint Analysis.

b) En **Procesos que se van a cancelar**, introduzca el proceso.

Especifica los procesos que debe detener el complemento Endpoint Analysis.

c) En **Archivos que se van a eliminar**, introduzca el nombre del archivo.

Especifica los archivos que debe eliminar el complemento Endpoint Analysis. Al eliminar o cancelar un proceso, se muestra una notificación a los usuarios finales.



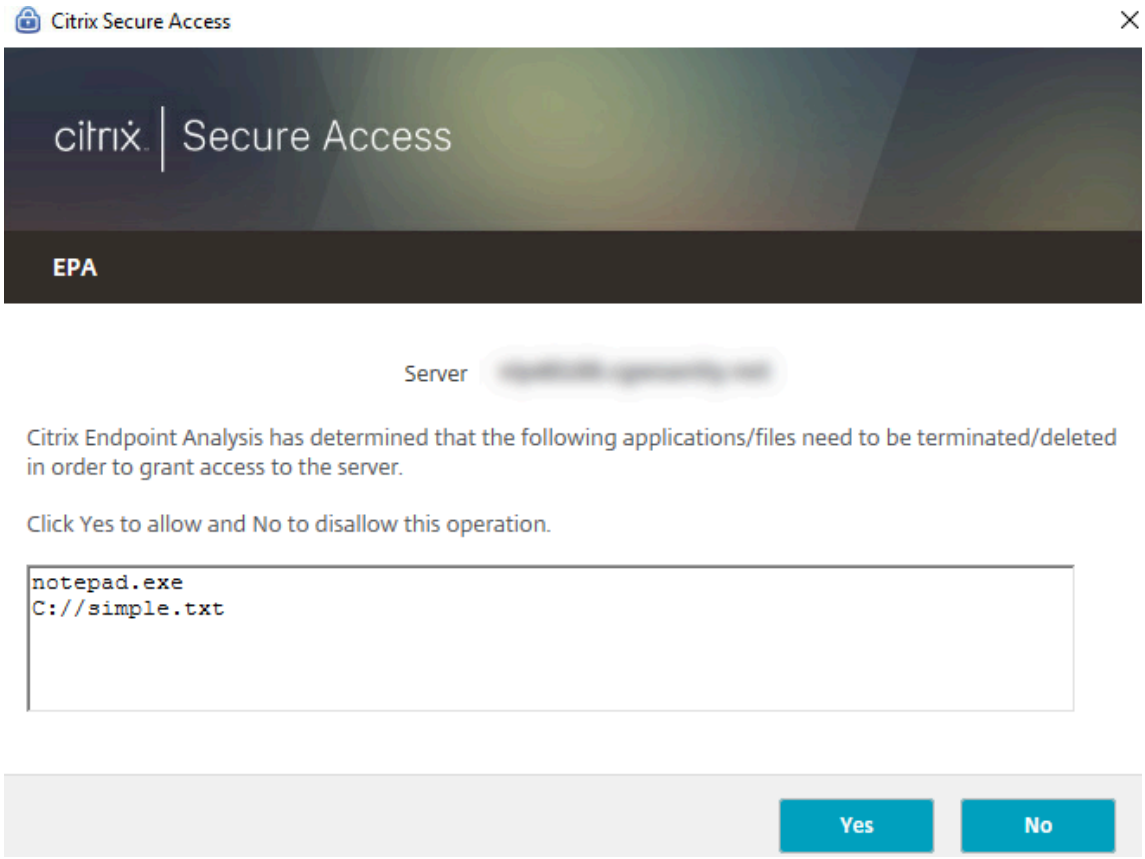
4. En Expresión, puede dejar la expresión ns_true o crear una expresión para una aplicación específica, como un antivirus o un software de seguridad, y, a continuación, hacer clic en **Aceptar**.

Para configurar un perfil de preautenticación mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Políticas > Autenticación/autorización** y, a continuación, haga clic en **Pre-Autenticación EPA**.
2. En el panel de detalles, en la pestaña **Perfiles** , haga clic en **Agregar** .
3. En **Nombre**, escriba el nombre de la aplicación que se va a comprobar.
4. En **Acción**, selecciona **PERMITIR** o **DENEGAR**.
5. En **Procesos que se van a cancelar**, escriba el nombre del proceso que se va a detener.

6. En **Archivos que se van a eliminar**, escriba el nombre del archivo que se va a eliminar, como c:\clientext.txt, haga clic en **Crear y, a continuación,** haga clic en **Cerrar**.

   Especifica los archivos que debe eliminar el complemento Endpoint Analysis. Al eliminar o cancelar un proceso, se muestra una notificación a los usuarios finales.



Si usa la GUI para configurar un perfil de preautenticación, cree la directiva de preautenticación haciendo clic en **Agregar** en la ficha **Directivas**. En el cuadro de diálogo **Crear directiva de preautenticación**, seleccione el perfil en el menú **Perfil de solicitud**.

Agregar una expresión preconfigurada a una directiva de preautenticación

NetScaler Gateway incluye expresiones preconfiguradas, denominadas expresiones con nombre. Al configurar una directiva, puede utilizar una expresión con nombre para la directiva. Por ejemplo, quiere que la directiva de preautenticación compruebe la existencia de Symantec antivirus 10 con definiciones de virus actualizadas. Cree una directiva de preautenticación y agregue la expresión tal y como se describe en el procedimiento siguiente.

Al crear una directiva de sesión o preautenticación, puede crear la expresión al crear la directiva. A continuación, puede aplicar la directiva, con la expresión, a servidores virtuales o de forma global.

En el procedimiento siguiente se describe cómo agregar una expresión antivirus preconfigurada a una directiva mediante la utilidad de configuración.

Agregar una expresión con nombre a una directiva de preautenticación

1. Vaya a **NetScaler Gateway > Políticas > Autenticación/autorización** y, a continuación, haga clic en **Pre-Autenticación EPA**.
2. En el panel de detalles, seleccione una directiva y, a continuación, haga clic en **Abrir**.
3. Junto a **Expresiones con nombre**, seleccione **Antivirus**y seleccione el producto antivirus de la lista.
4. Haga clic en **Agregar expresión**, haga clic en **Crear y,** a continuación, en **Cerrar**.

Configurar expresiones personalizadas

Una expresión personalizada es aquella que se crea dentro de la directiva. Al crear una expresión, configura los parámetros de la expresión.

También puede crear expresiones personalizadas para hacer referencia a las cadenas utilizadas con más frecuencia. Esto facilita el proceso de configuración de directivas de preautenticación y también el mantenimiento de las expresiones configuradas.

Por ejemplo, quiere crear una expresión personalizada para Symantec Antivirus 10 y asegurarse de que las definiciones de virus no tengan más de tres días de antigüedad. Cree una directiva y, a continuación, configure la expresión para especificar las definiciones de virus.

El procedimiento siguiente muestra cómo crear una expresión en una directiva de preautenticación. Puede seguir los mismos pasos en una directiva de sesión.

Cree una directiva de preautenticación y una expresión personalizada

1. **Vaya a**NetScaler Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Autenticación**EPA.**
2. En el panel de detalles, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En el cuadro de diálogo Crear perfil de autenticación, en **Nombre**, escriba un nombre para el perfil y, en **Acción**, seleccione **Permitir** y, a continuación, haga clic en **Crear**.
6. En el cuadro de diálogo Crear directiva de autenticación previa, junto a Coincidir con**cualquier expresión**, haga clic en **Agregar**.
7. En **Tipo de expresión**, seleccione **Seguridad del cliente**.
8. Configure las siguientes opciones:

a) En **Componente**, seleccione **Antivirus**.
b) En **Nombre**, escriba un nombre para la aplicación.
c) En **Qualifier**, selecciona **Versión**.
d) En **Operador**, seleccione **==**.
e) En **Valor**, escriba el valor.
f) En **Freshness**, escriba 3 y, a continuación, haga clic en **Aceptar**.

9. En el cuadro de diálogo Crear directiva de preautenticación, haga clic en **Crear** y, a continuación, en **Cerrar**.

Al configurar una expresión personalizada, se agrega al cuadro **Expresión** del cuadro de diálogo de la directiva.

Configurar expresiones compuestas

Una directiva de preautenticación puede tener un perfil y varias expresiones. Si configura expresiones compuestas, utiliza operadores para especificar las condiciones de la expresión. Por ejemplo, puede configurar expresiones compuestas para exigir que el dispositivo del usuario ejecute una de las siguientes aplicaciones antivirus:

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

La expresión se configura con el operador OR para comprobar las tres aplicaciones anteriores. Si NetScaler Gateway detecta la versión correcta de alguna de las aplicaciones del dispositivo del usuario, los usuarios pueden iniciar sesión. La expresión del cuadro de diálogo de directivas aparece de la siguiente manera:

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

Para obtener más información sobre las expresiones compuestas, consulte Configuración de expresiones compuestas.

Enlazar directivas de preautenticación

Después de crear la directiva de preautenticación, vincule la directiva al nivel al que se aplica. Puede enlazar las directivas de preautenticación a servidores virtuales o de forma global.

Crear y enlazar una directiva de preautenticación de forma global

1. En la ficha Configuración, haga clic en **NetScaler Gateway** y, a continuación, en **Configuración global**.

2. En el panel de detalles, haga clic en **Cambiar la configuración de preautenticación**.
3. En el cuadro de diálogo Configuración global de preautenticación, en **Acción**, seleccione **Permitir** o **Denegar**.
4. En **Nombre**, escriba un nombre para la directiva.
5. En el cuadro de diálogo **Configuración de preautenticación global**, junto a **Expresiones con nombre**, seleccione **General**, valor **True**, haga clic en **Agregar expresión**, haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Enlazar una directiva de preautenticación a un servidor virtual

1. En la ficha Configuración, haga clic en **NetScaler Gateway** y, a continuación, en **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y haga clic en **Open**.
3. En el cuadro de diálogo configurar el servidor virtual de NetScaler Gateway, haga clic en la ficha **Directivas** y, a continuación, en **Preautenticación**.
4. En Detalles, haga clic en **Insertar directiva**y, a continuación, en Nombre de directiva, seleccione la directiva de preautenticación.
5. Haga clic en **Aceptar**.

Desvincular y quitar directivas de preautenticación

Si es necesario, puede quitar una directiva de preautenticación de NetScaler Gateway. Antes de quitar una directiva de preautenticación, desvincúlelo del servidor virtual o de forma global.

Desvincular una directiva global de preautenticación

1. Vaya a **NetScaler Gateway > Políticas > Autenticación/autorización** y, a continuación, haga clic en **Pre-Autenticación EPA**.
2. En el panel de detalles, seleccione una directiva y, a continuación, en **Acción**, haga clic en **Enlaces globales**.
3. En el cuadro de diálogo **Vincular o desvincular directivas de preautenticación a global**, seleccione una directiva, haga clic en **Desvincular directiva**y, a continuación, haga clic en **Aceptar**.

Desvincular una directiva de preautenticación de un servidor virtual

1. En la ficha Configuración, haga clic en **NetScaler Gateway** y, a continuación, en **Servidores virtuales**.
2. En el cuadro de diálogo **Configurar servidor virtual de NetScaler Gateway**, haga clic en la ficha **Directivas** y, a continuación, en **Preautenticación**.

3. Seleccione la directiva y, a continuación, haga clic en **Desvincular directiva**.

Cuando la directiva de preautenticación es independiente, puede quitarla de NetScaler Gateway.

Quitar una directiva de preautenticación

1. **Vaya a**NetScaler Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Autenticación**EPA.**
2. en el panel de detalles, seleccione una directiva y, a continuación, haga clic en **Eliminar**.

Establecer la prioridad de las directivas de preautenticación

Puede tener varias directivas de preautenticación vinculadas a distintos niveles. Por ejemplo, tiene una directiva que comprueba si una aplicación antivirus específica está enlazada globalmente y una directiva de firewall vinculada al servidor virtual. Cuando los usuarios inician sesión, se aplica primero la directiva vinculada al servidor virtual. La directiva que está vinculada a nivel mundial se aplica en segundo lugar.

Puede cambiar el orden en que se realizan los análisis de preautenticación. Para que NetScaler Gateway aplique primero la directiva global, cambie el número de prioridad de la directiva vinculada al servidor virtual, asignándole un número de prioridad superior al de la directiva vinculada globalmente. Por ejemplo, establezca el número de prioridad de la directiva global en uno y la directiva del servidor virtual en dos. Cuando los usuarios inician sesión, NetScaler Gateway ejecuta primero el análisis de directivas globales y, en segundo lugar, el análisis de directivas del servidor virtual.

Cambiar la prioridad de una directiva de preautenticación

1. En la ficha Configuración, haga clic en **NetScaler Gateway** y, a continuación, en **Servidores virtuales**.
2. En el panel de detalles, seleccione un servidor virtual y haga clic en **Open**.
3. En la ficha Directivas, haga clic en **Autenticación previa**.
4. En Prioridad, escriba el número de prioridad de la directiva y, a continuación, haga clic en **Aceptar**.

Directivas posteriores a la autenticación

March 27, 2024

> **Importante:**
>
> El objetivo de Endpoint Analysis es analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no hace cumplir ni validar la seguridad de los dispositivos de los usuarios finales. Se recomienda utilizar sistemas de seguridad de dispositivos de punto final para proteger los dispositivos de los ataques de los administradores locales.

Una directiva posterior a la autenticación es un conjunto de reglas genéricas que el dispositivo del usuario debe cumplir para mantener activa la sesión. Si se produce un error en la directiva, finaliza la conexión con NetScaler Gateway. Al configurar la directiva posterior a la autenticación, puede configurar cualquier configuración para las conexiones de usuario que se puedan hacer condicionales.

Las directivas de sesión se utilizan para configurar directivas posteriores a la autenticación. En primer lugar, crea los usuarios a los que se aplica la directiva. A continuación, agregará los usuarios a un grupo. A continuación, enlazará las aplicaciones de sesión, directivas de tráfico e intranet al grupo.

También puede especificar que los grupos sean grupos de autorización. Este tipo de grupo permite asignar usuarios a grupos en función de una expresión de verificación del dispositivo cliente dentro de la directiva de sesión.

También puede configurar una directiva posterior a la autenticación para poner a los usuarios en un grupo de cuarentena si el dispositivo de usuario no cumple los requisitos de la directiva. Una directiva simple incluye una expresión de comprobación del dispositivo cliente y un mensaje. Cuando los usuarios están en el grupo de cuarentena, los usuarios pueden iniciar sesión en NetScaler Gateway; sin embargo, tienen acceso limitado a los recursos de red.

No se puede crear un grupo de autorización ni un grupo de cuarentena mediante el mismo perfil y directiva de sesión. Los pasos para crear la directiva posterior a la autenticación son los mismos. Al crear la directiva de sesión, selecciona un grupo de autorización o un grupo de cuarentena. Puede crear dos directivas de sesión y vincular cada directiva al grupo.

Las directivas posteriores a la autenticación también se utilizan con SmartAccess. Para obtener más información sobre SmartAccess, consulte Configuración de SmartAccess en NetScaler Gateway.

> **Nota:**
>
> Esta funcionalidad solo funciona con el cliente Citrix Secure Access. Si los usuarios inician sesión con la aplicación Citrix Workspace, el análisis de Endpoint Analysis se ejecuta solo al iniciar sesión.

Configurar una directiva posterior a la autenticación

Se utiliza una directiva de sesión para configurar una directiva posterior a la autenticación. Una directiva simple incluye una expresión de comprobación del dispositivo cliente y un mensaje.

Para configurar una directiva posterior a la autenticación mediante la interfaz gráfica de usuario

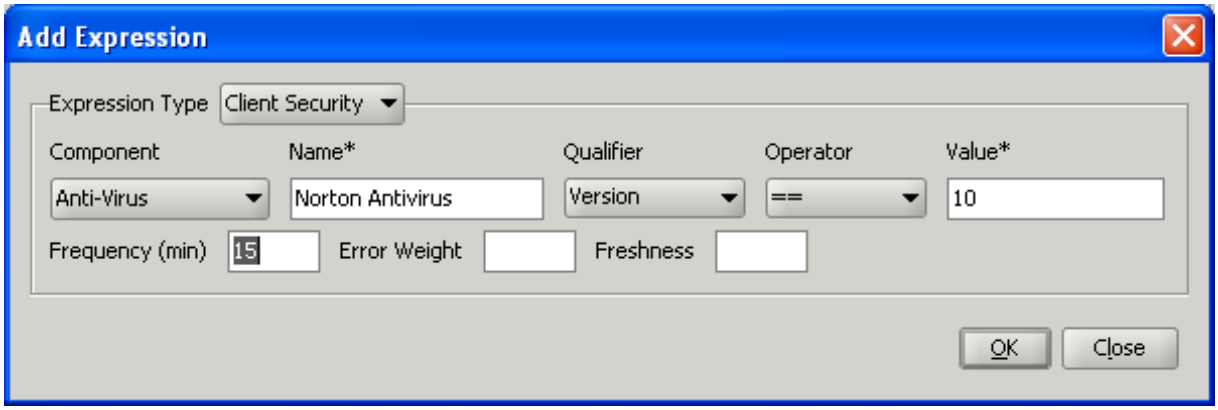
1. Expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha Seguridad, haga clic en **Configuración avanzada**.
7. En **Seguridad del cliente**, haga clic en **Supedición global y,** a continuación, haga clic en **Nuevo**.
8. Configure la expresión de comprobación del dispositivo cliente y, a continuación, haga clic en **Crear**.
9. En **Seguridad del cliente**, en Grupo de cuarentena, seleccione un grupo.
10. En **Mensaje de error**, escriba el mensaje que desea que reciban los usuarios si falla el análisis posterior a la autenticación.
11. En Grupos de autorización, haga clic en **Sobrescribir global**, seleccione un grupo, haga clic en **Agregar**, haga clic en **Aceptar** y, a continuación, haga clic en **Crear**.
12. En el cuadro de diálogo **Crear directiva de sesión**, junto a Expresiones con nombre, seleccione **General**, seleccione **Valor verdadero**, haga clic en **Agregar expresión**, en **Crear** y, a continuación, en **Cerrar**.

Configurar la frecuencia de los análisis posteriores a la autenticación

Puede configurar NetScaler Gateway para que ejecute la directiva posterior a la autenticación a intervalos especificados. Por ejemplo, configuró una directiva de verificación del dispositivo cliente y desea que se ejecute en el dispositivo del usuario cada 10 minutos. Puede configurar esta frecuencia mediante la creación de una expresión personalizada dentro de la directiva.

> **Nota:**
>
> La función de comprobación de frecuencia para las directivas posteriores a la autenticación solo funciona con el cliente Citrix Secure Access. Si los usuarios inician sesión con la aplicación Citrix Workspace, el análisis de Endpoint Analysis se ejecuta solo al iniciar sesión.

Puede establecer la frecuencia (en minutos) al configurar la directiva de verificación del dispositivo cliente siguiendo el procedimiento Configuración de una directiva de posautenticación. La siguiente figura muestra dónde puede introducir un valor de frecuencia en el cuadro de diálogo **Agregar expresión** .



Grupos de cuarentena y autorización

Cuando los usuarios inician sesión en NetScaler Gateway, los asigna a un grupo que configura en NetScaler Gateway o en un servidor de autenticación de la red segura. Si un usuario falla un análisis posterior a la autenticación, puede asignarlo a un grupo restringido, denominado grupo de cuarentena, que restringe el acceso a los recursos de red.

También puede utilizar grupos de autorización para restringir el acceso de los usuarios a los recursos de red. Por ejemplo, es posible que un grupo de personal contratado tenga acceso únicamente a su servidor de correo electrónico y a un recurso compartido de archivos. Cuando los dispositivos de usuario superan los requisitos de verificación de dispositivos que definió en NetScaler Gateway, los usuarios pueden convertirse en miembros de grupos de forma dinámica.

Utilice la configuración global o las directivas de sesión para configurar grupos de cuarentena y autorización vinculados a un usuario, grupo o servidor virtual. Puede asignar usuarios a grupos en función de una expresión de verificación del dispositivo cliente dentro de la directiva de sesión. Cuando el usuario es miembro de un grupo, NetScaler Gateway aplica la directiva de sesión basada en la pertenencia al grupo.

Configurar grupos de autorización

Al configurar un análisis de Endpoint Analysis, puede agregar usuarios de forma dinámica a un grupo de autorización cuando el dispositivo de usuario supera el análisis. Por ejemplo, crea un análisis de Endpoint Analysis que comprueba la pertenencia al dominio del dispositivo de usuario. En NetScaler Gateway, cree un grupo local denominado Equipos unidos a un dominio y agréguelo como grupo de autorización para cualquier persona que supere el análisis. Cuando los usuarios se unen al grupo, los usuarios heredan las directivas asociadas al grupo.

No se pueden enlazar directivas de autorización de forma global ni a un servidor virtual. Puede utilizar grupos de autorización para proporcionar un conjunto predeterminado de directivas de autorización cuando los usuarios no están configurados para ser miembros de otro grupo en NetScaler Gateway.

Para configurar un grupo de autorización mediante una directiva de sesión

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha Seguridad, haga clic en **Configuración avanzada**.
7. En Grupos de autorización, haga clic en **Supeditar global** y seleccione un grupo de la lista desplegable.
8. Haga clic en **Agregar**, en **Aceptar** y, a continuación, en **Crear**.
9. En el cuadro de diálogo **Crear política de sesión** , junto a Expresiones con nombre, seleccione **General** , seleccione **Valor verdadero** , haga clic en **Agregar expresión** , en **Crear y,** a continuación, en **Cerrar** .

Después de crear la directiva de sesión, puede vincularla a un usuario, grupo o servidor virtual.

Para configurar un grupo de autorización global

1. Expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Configuración, haga clic en **Cambiar la configuración global**.
3. En la ficha Seguridad, haga clic en **Configuración avanzada**.
4. En Grupo de autorización, seleccione un grupo de la lista desplegable.
5. Haga clic en **Agregar** y, a continuación, en **Aceptar**.

Si desea eliminar un grupo de autorización de forma global o de la directiva de sesión, en el cuadro de diálogo Configuración de seguridad avanzada, seleccione el grupo de autorización de la lista y, a continuación, haga clic en **Eliminar**.

Configurar grupos de cuarentena

Al configurar un grupo de cuarentena, configura la expresión de verificación del dispositivo cliente mediante el cuadro de diálogo Configuración de seguridad: configuración avanzada de un perfil de sesión.

Para configurar la expresión de comprobación del dispositivo cliente para un grupo de cuarentena

1. Vaya a **NetScaler Gateway > Directivas** y haga clic en **Sesión**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.

5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha Seguridad, haga clic en **Configuración avanzada**.
7. En **Seguridad del cliente**, haga clic en **Supedición global y,** a continuación, haga clic en **Nuevo**.
8. En el cuadro de diálogo **Expresión de cliente**, configure la expresión de comprobación del dispositivo cliente y, a continuación, haga clic en **Crear**.
9. En **Grupo de cuarentena**, seleccione el grupo.
10. En Mensaje de error, escriba un mensaje que describa el problema para los usuarios y, a continuación, haga clic en **Crear**.
11. En el cuadro de diálogo **Crear directiva de sesión**, junto a Expresiones nombradas, seleccione **General**, seleccione **Valor verdadero** y haga clic en **Agregar expresión**.
12. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Después de crear la directiva de sesión, enlaza a un usuario, grupo o servidor virtual.

> **Nota:**
>
> Si se produce un error en el análisis de Endpoint Analysis y se coloca al usuario en el grupo de cuarentena, las directivas vinculadas al grupo de cuarentena solo surten efecto si no hay directivas vinculadas directamente al usuario que tengan un número de prioridad igual o inferior al de las directivas vinculadas al grupo de cuarentena.

Para configurar un grupo de cuarentena global

1. Expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en Configuración, haga clic en **Cambiar la configuración global**.
3. En la pestaña **Seguridad** , haz clic en **Configuración avanzada** .
4. En **Seguridad del cliente**, configure la expresión de comprobación del dispositivo cliente.
5. En **Grupo de cuarentena**, seleccione el grupo.
6. En **Mensaje de error**, escriba un mensaje que describa el problema para los usuarios y, a continuación, haga clic en **Aceptar**.

Expresiones de comprobación de dispositivos de preautenticación para dispositivos de usuario

March 27, 2024

> **Importante:**
>
> El objetivo de Endpoint Analysis es analizar el dispositivo del usuario según criterios de cumplim-

> iento predeterminados y no hace cumplir ni validar la seguridad de los dispositivos de los usuarios finales. Se recomienda utilizar sistemas de seguridad de dispositivos de punto final para proteger los dispositivos de los ataques de los administradores locales.

NetScaler Gateway proporciona varias comprobaciones de cumplimiento de los dispositivos de punto final durante el inicio de sesión del usuario o en otros momentos configurados durante una sesión que ayudan a validar los dispositivos de los usuarios. Solo los dispositivos de usuario que superen estas comprobaciones pueden establecer una sesión de NetScaler Gateway.

Los siguientes son los tipos de comprobaciones en los dispositivos de usuario que puede configurar en NetScaler Gateway:

- Antispam
- Antivirus
- Directivas de archivos
- Seguridad en Internet
- Sistema operativo
- Firewall personal
- Directivas de procesos
- Directivas de registro
- Directivas de servicio

Si se produce un error en la comprobación del dispositivo del usuario, no se establecería ninguna conexión nueva hasta que se supere una comprobación posterior (en el caso de comprobaciones que se realizan a intervalos regulares); sin embargo, el tráfico que fluye a través de las conexiones existentes sigue pasando por NetScaler Gateway.

Puede utilizar la utilidad de configuración para configurar directivas de autenticación previa o expresiones de comprobación de dispositivos dentro de las directivas de sesión diseñadas para realizar comprobaciones en los dispositivos de los usuarios.

Configurar expresiones antivirus, firewall, seguridad de Internet o antispam

Los ajustes de las directivas de antivirus, firewall, seguridad de Internet y antispam se configuran en el cuadro de diálogo **Agregar expresión** . La configuración de cada directiva es la misma: las diferencias son los valores que selecciona. Por ejemplo, si quiere comprobar en el dispositivo de usuario la versión 10 del antivirus Norton y ZoneAlarm Pro, cree dos expresiones dentro de la directiva de sesión o autenticación previa que especifican el nombre y el número de versión de cada aplicación.

Al seleccionar Seguridad del cliente como tipo de expresión, puede configurar lo siguiente:

- Componente: tipo de seguridad del cliente, como antivirus, firewall o entrada de registro.
- Nombre: Nombre de la aplicación, proceso, archivo, entrada de registro o sistema operativo.

- Calificador: la versión o el valor del componente que comprueba la expresión.
- Operador: comprueba si el valor existe o es igual al valor.
- Valor: versión de la aplicación para antivirus, firewall, seguridad de Internet o software antispam en el dispositivo del usuario.
- Frecuencia: Frecuencia con la que se ejecuta un análisis posterior a la autenticación, en minutos.
- Peso del error: ponderación asignada a cada mensaje de error contenido en una expresión anidada cuando varias expresiones tienen cadenas de error diferentes. El peso determina qué mensaje de error aparece.
- Frescura: define la antigüedad de una definición de virus. Por ejemplo, puede configurar la expresión para que las definiciones de virus no tengan más de tres días.

Para agregar una directiva de verificación del dispositivo cliente a una directiva de preautenticación o de sesión

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:

    a) **En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda**NetScaler Gateway > Directivas**y, a continuación, haga clic en Sesión.**
    b) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Políticas > Autenticación/autorización** y, a continuación, haga clic en **Pre-Autenticación EPA** .

2. En el panel de detalles, en la pestaña Políticas, haga clic en **Agregar** .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione **Seguridad del cliente**.
6. Configure los ajustes para lo siguiente:

    a) En Componente, seleccione el elemento que quiere escanear.
    b) En Nombre, escriba el nombre de la aplicación.
    c) En Qualifier, selecciona **Versión** .
    d) En Operador, seleccione el valor.
    e) En Valor, escriba la cadena de verificación del dispositivo cliente, haga clic en **Aceptar**, en **Crear** y, a continuación, en **Cerrar**.

Configurar directivas de servicio

Un servicio es un programa que se ejecuta de forma silenciosa en el dispositivo del usuario. Al crear una directiva de sesión o de autenticación previa, puede crear una expresión que garantice que los dispositivos de usuario ejecuten un servicio determinado cuando se establece la sesión.

Para configurar una directiva de servicio

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a) En la utilidad de configuración, en la pestaña Configuración, en el panel de navegación, expanda **NetScaler Gateway > Políticas** y, a continuación, haga clic en Sesión.
    b) En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas > Autenticación/autorización y, a continuación, haga clic en Pre-Autenticación EPA**.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:
    a) En Componente, seleccione Servicio.
    b) En Nombre, escriba el nombre del servicio.
    c) En Calificador, déjalo en blanco o selecciona Versión.
    d) En función de su selección en Qualifier, realiza una de las siguientes acciones:
        - Si se deja en blanco, en Operador, seleccione == o! =
        - Si ha seleccionado Versión, en Operador, en Valor, escriba el valor, haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Puede consultar una lista de todos los servicios disponibles y el estado de cada uno de ellos en un equipo basado en Windows en la siguiente ubicación:

Panel de control > Herramientas administrativas > Servicios

> **Nota:**
>
> El nombre del servicio de cada servicio varía del nombre que aparece en la lista. Compruebe el nombre del servicio en el cuadro de diálogo
> Propiedades.

Configurar directivas de procesos

Al crear una directiva de sesión o de autenticación previa, puede definir una regla que exija que todos los dispositivos de usuario tengan un proceso concreto ejecutándose cuando los usuarios inicien sesión. El proceso puede ser cualquier aplicación y puede incluir aplicaciones personalizadas.

Nota: La lista de todos los procesos que se ejecutan en un equipo basado en Windows aparece en la ficha
Procesos del Administrador de tareas de Windows.

Para configurar una directiva de procesos

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:
    a) En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway\ > Directivas** y, a continuación, haga clic en Sesión.
    b) En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas \ > Autenticación/autorización** y, a continuación, haga clic en EPA previo a la autenticación.
2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:
    a) En Componente, seleccione Proceso.
    b) En Nombre, escriba el nombre de la aplicación.
    c) En Operador, seleccione EXISTS o NOTEXISTS, haga clic en Aceptar y, a continuación, en Cerrar.

Al configurar una directiva de Endpoint Analysis (autenticación previa o posterior a la autenticación) para comprobar si hay un proceso, puede configurar una suma de comprobación MD5.

Al crear la expresión de la directiva, puede agregar la suma de comprobación MD5 al proceso que está buscando. Por ejemplo, si está comprobando si notepad.exe se está ejecutando en el dispositivo del usuario, la expresión es:
CLIENT.APPLICATION.PROCESS (notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

Configurar directivas del sistema operativo

Al crear una directiva de sesión o preautenticación, puede configurar las cadenas de verificación del dispositivo cliente para determinar si el dispositivo del usuario ejecuta un sistema operativo determinado cuando los usuarios inician sesión. También puede configurar la expresión para que busque un service pack o una revisión concretos.

Los valores de Windows y Macintosh son:

Sistema operativo	Valor
macOS X	macOS
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7
Windows Vista	vista
Windows XP	`winxp`
Windows Server 2008	win2008
Windows Server 2003	win2003
Servidor Windows 2000	win2000
Plataforma Windows de 64 bits	win64

Para configurar una directiva del sistema operativo mediante la interfaz gráfica de usuario

1. En el panel de navegación, realice una de las siguientes acciones:
    a) Vaya a **NetScaler Gateway > Directivas** y haga clic en **Sesión**.
    b) Vaya a **NetScaler Gateway > Directivas > Autenticación previa**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. En **Solicitar acción**, seleccione una acción existente o cree una.
5. Haga clic en **Editor de expresiones**.
6. En **Seleccionar tipo de expresión**, seleccione **Seguridad del cliente**.
7. Configure los ajustes para lo siguiente:
    a) En **Componente**, seleccione **Sistema operativo**.
    b) En **Nombre**, escriba el nombre del sistema operativo.
    c) En Qualifier, realiza una de las siguientes acciones:

- Deja el campo en blanco
- Seleccione **Service Pack**
- Seleccionar **revisión**
- Seleccionar **versión** (solo para macOS)

d) Según lo que haya seleccionado en el paso 7, en Operador, realice una de las siguientes acciones:

- Si Qualifier está en blanco, en Operador, seleccione EQUAL (= =), NOTEQUAL (!=), EXISTS o NOTEXISTS.
- Si ha seleccionado Service Pack o Hotfix, seleccione el operador y, en Valor, escriba el valor.

8. Haga clic en **Listo** y luego en **Cerrar**.

Si está configurando un service pack, como client.os (`winxp`).`sp`, si no hay un número en el campo **Valor**, NetScaler Gateway devuelve un mensaje de error porque la expresión no es válida.

Si el sistema operativo tiene Service Pack presentes, como Service Pack 3 y Service Pack 4, puede configurar una comprobación solo para Service Pack 4, ya que la presencia de Service Pack 4 indica automáticamente que los Service Pack anteriores están presentes.

Configurar directivas de registro

Al crear una directiva de sesión o de autenticación previa, puede comprobar la existencia y el valor de las entradas del registro en el dispositivo del usuario. La sesión se establece solo si la entrada en particular existe o tiene el valor configurado o superior.

Al configurar una expresión de registro, siga las siguientes pautas:

- Se utilizan cuatro barras diagonales inversas para separar claves y subclaves, como

  HKEY_LOCAL_MACHINE\\\\ SOFTWARE

- Los guiones bajos se utilizan para separar la subclave y el nombre del valor asociado, como

  HKEY_LOCAL_MACHINE\\\\ SOFTWARE\\\\ VIRUSSOFTWARE_VERSION

- Se utiliza una barra diagonal inversa (\) para indicar un espacio, como en los dos ejemplos siguientes:

  HKEY_LOCAL_MACHINE\\\\ SOFTWARE\\ Citrix\\\\ Secure\ Access\ Client_ProductVersion

  CLIENT.REG (HKEY_LOCAL_MACHINESOftwareSymantecNorton Antivirus_Version).VALUE == 12.8.0.4 -frecuencia 5

La siguiente es una expresión de registro que busca la clave de registro del cliente Citrix Secure Access cuando los usuarios inician sesión:

CLIENT.REG(`secureaccess`).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client

> **Nota:**
>
> Si busca claves y valores del Registro, y selecciona Formato libre avanzado en el cuadro de diálogo de expresión, la expresión debe empezar por CLIENT.REG.

Las comprobaciones de registro se admiten en los cinco tipos más comunes siguientes:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Los valores de registro que se van a comprobar utilizan los siguientes tipos:

- Cadena

  Para el tipo de valor de cadena, se comprueba que se distinga entre mayúsculas

- DWORD

  Para el tipo DWORD, el valor se compara y debe ser igual.

- Cadena expandida

  Otros tipos, como binario y multicadena, no son compatibles.

- Solo se admite el operador de comparación '=='.
- No se admiten otros operadores de comparación, como <, > y comparaciones que distinguen mayúsculas y minúsculas.
- La longitud total de la cadena de registro debe ser inferior a 256 bytes.

Puede agregar un valor a la expresión. El valor puede ser una versión de software, una versión del service pack o cualquier otro valor que aparezca en el registro. Si el valor de datos del registro no coincide con el valor con el que se realiza la prueba, se deniega el inicio de sesión a los usuarios.

> **Nota:**
>
> No se puede buscar un valor dentro de una subclave. El análisis debe coincidir con el valor nombrado y el valor de datos asociado.

Para configurar una directiva de registro

1. En la utilidad de configuración, en el panel de navegación, realice una de las siguientes acciones:

a) En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway\ > Directivas** y, a continuación, haga clic en Sesión.
b) En la utilidad de configuración, en la ficha Configuración, en el panel de navegación, expanda **NetScaler Gateway > Directivas \ > Autenticación/autorización** y, a continuación, haga clic en EPA previo a la autenticación.

2. En el panel de detalles, en la pestaña Políticas, haga clic en Agregar .
3. En Nombre, escriba un nombre para la directiva.
4. Junto a Coincidir con cualquier expresión, haga clic en Agregar.
5. En el cuadro de diálogo Agregar expresión, en Tipo de expresión, seleccione Seguridad del cliente.
6. Configure los ajustes para lo siguiente:

a) En Componente, seleccione Registro.
b) En Nombre, escriba el nombre de la clave de registro.
c) En Calificador, déjalo en blanco o selecciona Valor.
d) En Operador, realice una de las siguientes acciones:
- Si el calificador se deja en blanco, seleccione EXISTS o NOTEXISTS
- Si ha seleccionado Valor en Calificador, seleccione == o !==

e) En Valor, escriba el valor tal y como aparece en el editor del registro, haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Configurar expresiones de comprobación compuestas del dispositivo cliente

Puede combinar cadenas de verificación del dispositivo cliente para formar expresiones de comprobación compuestas del dispositivo cliente.

Los operadores booleanos compatibles con NetScaler Gateway son:

- Y (&&)

O bien (

-

- No (!)

Para mayor precisión, puede agrupar las cadenas entre paréntesis.

> **Nota:**
>
> Si utiliza la línea de comandos para configurar expresiones, utilice paréntesis para agrupar las expresiones de comprobación del dispositivo cuando forme una expresión compuesta. El uso

> de paréntesis mejora la comprensión y depuración de la expresión del cliente.

Configurar directivas con el operador AND (&&)

El operador AND (&&) funciona combinando dos cadenas de verificación del dispositivo cliente para que la comprobación compuesta solo se apruebe cuando ambas comprobaciones son verdaderas. La expresión se evalúa de izquierda a derecha y, si la primera comprobación falla, no se lleva a cabo la segunda comprobación.

Puede configurar el operador AND (&&) mediante la palabra clave "AND"o los símbolos "&&".

Ejemplo:

Esto es una comprobación del dispositivo cliente que determina si el dispositivo del usuario tiene instalada y en ejecución la versión 7.0 del antivirus de Sophos. También comprueba si el servicio Inicio de sesión en red se está ejecutando en el mismo equipo.

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon)
EXISTS
```

Esta cadena también se puede configurar como:

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon)
EXISTS
```

Configurar directivas con el operador OR (||)

El operador OR (||) funciona mediante la combinación de dos cadenas de verificación del dispositivo. La comprobación compuesta se aprueba cuando cualquiera de las dos comprobaciones es verdadera. La expresión se evalúa de izquierda a derecha y, si se aprueba la primera comprobación, no se lleva a cabo la segunda comprobación. Si no se aprueba la primera comprobación, se realiza la segunda comprobación.

Puede configurar el operador OR (||) mediante la palabra clave OR o el símbolo ||.

Ejemplo:

La siguiente es una comprobación del dispositivo cliente que determina si el dispositivo del usuario contiene el archivo c:\\file.txt o el proceso putty.exe en ejecución.

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)OR (client.proc(putty.exe)
EXISTS
```

Esta cadena también se puede configurar como

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)|| (client.proc(putty.exe)
EXISTS
```


Configurar directivas mediante el comando NOT (!) operador

El operador NOT (!) o de negación niega la cadena de verificación del dispositivo cliente.

Ejemplo:

La siguiente comprobación del dispositivo cliente se realiza si el archivo c:\sophos_virus_defs.dat file NO tiene más de dos días:

```
\!(client.file(c:\\\\\\\\\\sophos\\_virus\\_defs.dat).timestamp==2dy)
```

El escaneo EPA como factor en la autenticación nFactor

March 27, 2024

> **Importante:**
>
> El objetivo de Endpoint Analysis es analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no hace cumplir ni validar la seguridad de los dispositivos de los usuarios finales. Se recomienda utilizar sistemas de seguridad de dispositivos de punto final para proteger los dispositivos de los ataques de los administradores locales.

Las siguientes son algunas de las entidades básicas de nFactor EPA.

Acción de EPA: Una acción de EPA es un tipo de acción introducido para EPA de nFactor. Contiene lo siguiente:

- Expresión de comprobación del dispositivo cliente: Esta expresión se envía al plug-in de EPA de Gateway para su evaluación.
- Grupo de éxito: Este grupo, si está configurado, se hereda en la sesión de Gateway si el resultado de EPA es verdadero.
- Grupo de cuarentena: Este grupo, si está configurado, se hereda en la sesión de Gateway si el resultado de EPA es falso.
- killProcess: Representa el nombre del proceso que el proceso de EPA debe detener.
- deleteFiles: Especifica las rutas separadas por comas a los archivos que el proceso de EPA debe eliminar.

Los grupos se pueden utilizar durante la duración de la sesión para determinar si el cliente cumple determinadas condiciones de la EPA.
Si en un factor determinado, EPA falla, la última acción no contiene el "Grupo de cuarentena"y se da por finalizada la autenticación de ese usuario.

Si existe un "grupo en cuarentena", se continúa con la autenticación y el administrador puede comprobar si el grupo otorga acceso limitado. Para obtener más información, consulte Ejecución de la EPA.

Directiva de EPA: En nFactor, todas las directivas se agregar con la misma sintaxis "add authentication policy". Sin embargo, el tipo de acción califica a la directiva como directiva de la EPA.

Factor de EPA: El factor de EPA es una etiqueta de directiva habitual. No existe ninguna entidad denominada factor EPA. Una vez que la directiva de la EPA está vinculada a un factor, hereda ciertas propiedades que la convierten en un factor EPA.

> **Nota:**
>
> El término "factor de EPA"se usa comúnmente en este documento para referirse a un factor incluido en las directivas de EPA.

EPA —Cuarentena: Si, en un factor determinado, fallan todas las expresiones de comprobación del dispositivo cliente de todas las acciones y, si la última acción contiene un "grupo en cuarentena", ese grupo se agrega a la sesión y se analiza el nextFactor. Es decir, a pesar del fracaso, la presencia del "grupo de cuarentena"califica la sesión para la siguiente etapa. Sin embargo, debido a la herencia de un grupo especial, el administrador puede relegar la sesión al acceso restringido o a directivas de autenticación adicionales como OTP o SAML.

Si no hay ningún grupo de cuarentena en la última acción, la autenticación finaliza en caso de error.

La EPA en nFactor también utiliza las siguientes entidades:

- **LoginSchema:** Representación XML del formulario de inicio de sesión. Define la "vista"del formulario de inicio de sesión y también tiene las propiedades de un "factor".
- **Etiqueta de directiva o factor de directiva:** Es un conjunto de directivas que se prueban en una etapa determinada de la autenticación.
- **Etiqueta de servidor virtual:** El servidor virtual también es una etiqueta de directiva, es decir, se pueden vincular directivas al servidor virtual. Sin embargo, el servidor virtual es la colección de varias etiquetas de directivas, ya que es el punto de entrada para el acceso de los usuarios.
- **next factor:** Se utiliza para especificar la etiqueta/factor de la directiva que se utilizará una vez que la directiva de autenticación dada se haya aplicado correctamente.
- **Directiva NO_AUTHN:** Directiva especial cuya acción siempre se realiza correctamente.
- **Factor de PassThrough:** Es una etiqueta o factor de directiva cuyo esquema de inicio de sesión no contiene ninguna vista. Es una indicación para que el dispositivo NetScaler continúe la autenticación en el factor determinado sin la intervención del usuario.

Para obtener más información, consulte Conceptos, entidades y terminología de nFactor.

Exclusividad mutua EPA Factor

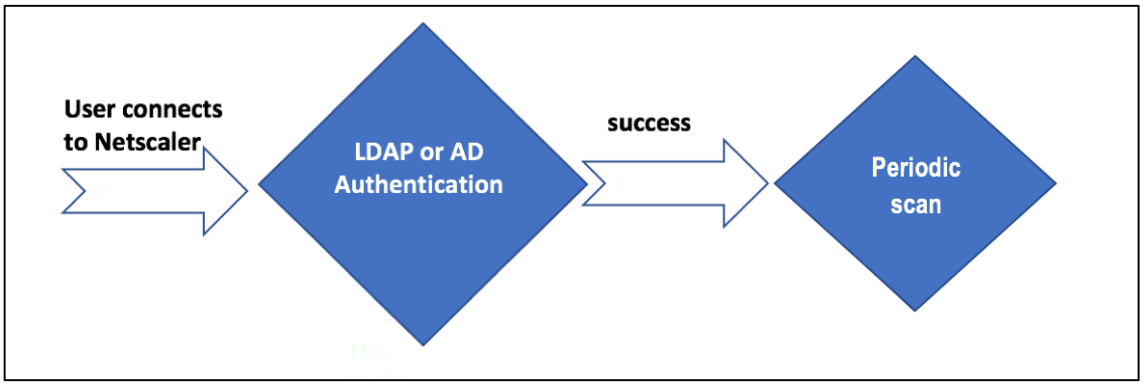
EPA Factor contiene una o más directivas de la EPA. Una vez que las directivas de la EPA están vinculadas a un factor, las directivas de autenticación regulares no se permiten en ese factor. Esta restricción es ofrecer la mejor experiencia de usuario y una separación clara del análisis de endpoints. La única excepción a esta regla es la directiva NO_AUTHN. Dado que la directiva NO_AUTHN es una directiva especial que se utiliza para simular "on-failure-jump", está permitida en el factor de EPA.

Ejecución de la EPA

En cualquier factor (incluido el factor servidor virtual), antes de entregar el formulario de inicio de sesión, el dispositivo NetScaler comprueba si el factor está configurado para EPA. Si es así, envía una respuesta específica al cliente (IU) para que se active la secuencia EPA. Esta secuencia comprende que el cliente solicite expresiones de verificación del dispositivo cliente y envíe los resultados.
Las expresiones de verificación del dispositivo cliente para todas las directivas de un factor se envían al cliente a la vez. Una vez que se obtienen los resultados en el dispositivo NetScaler, cada una de las expresiones de todas las acciones se evalúan en una secuencia. La primera acción que da como resultado el éxito de la EPA termina ese factor y DefaultGroup, si está configurado, se hereda en la sesión. Si se encuentra la directiva NO_AUTHN, se califica como automática correcta. Si se especifica nextFactor, el dispositivo continúa con ese factor. De lo contrario, la autenticación finaliza.
Esta condición también se aplica al primer factor. Si no hay ningún factor de directiva de autenticación después de EPA en el servidor virtual, la autenticación finaliza. Esto es diferente del comportamiento de las directivas clásicas, en el que al usuario siempre se le muestra la página de inicio de sesión después de la EPA.
Sin embargo, en caso de que no haya una directiva EPA correcta, NetScaler Gateway examina el grupo de cuarentena configurado para la última directiva de EPA en ese factor o en cascada. Si la última directiva está configurada con el grupo de cuarentena, ese grupo se agrega a la sesión y se inspecciona el NextFactor. Si existe un NextFactor, la autenticación pasa a ese factor. De lo contrario, se completará la autenticación.

Configurar el escaneo de EPA para que se ejecute después de la autenticación

Puede configurar el escaneo de EPA para que se ejecute después de la autenticación. En el siguiente ejemplo, el escaneo de EPA se utiliza como comprobación final en una autenticación nFactor o de varios factores. En esta configuración, si el escaneo de EPA falla durante alguna de estas comprobaciones, la sesión finaliza.



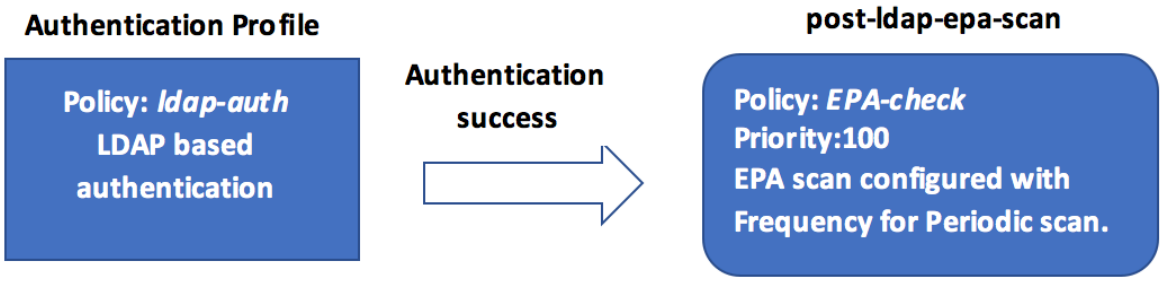
- El usuario intenta conectarse a la IP virtual de NetScaler Gateway.
- Se muestra al usuario una página de inicio de sesión con el campo de nombre de usuario y contraseña para que proporcione sus credenciales de inicio de sesión. Con estas credenciales, la autenticación basada en LDAP o AD se realiza en el back-end. Si tiene éxito, se muestra al usuario una ventana emergente para autorizar el escaneo de la EPA.
- Una vez que el usuario lo autoriza, se realiza el análisis EPA y, en función del éxito o el fracaso de la configuración del cliente del usuario, se proporciona acceso.
- Si el escaneo se realiza correctamente, el escaneo de EPA se realiza periódicamente para comprobar que se siguen cumpliendo los requisitos de verificación del dispositivo configurados.
- Si se produce un error en el análisis de la EPA durante dicha comprobación, la sesión finaliza.

Requisitos previos

Se supone que existe la siguiente configuración:

- Configuración del servidor virtual de VPN, puerta de enlace y servidor virtual de autenticación
- Configuraciones del servidor LDAP y directivas asociadas.

En la siguiente sección se capturan las configuraciones de rótulos de directivas y directivas necesarias, así como la asignación de directivas y rótulos de directivas a un perfil de autenticación.



En la CLI

1. Cree una acción para realizar un análisis de la EPA antes de la autenticación de LDAP y asócielo a una directiva de análisis de la EPA.

```
add authentication epaAction pre-ldap-epa-action -csecexpr "sys.client_expr ("proc_2_firefox")"

add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-epa-action
<!--NeedCopy-->
```

   La expresión anterior analiza si el proceso "Firefox"se está ejecutando. El cliente de la EPA comprueba la existencia del proceso cada 2 minutos, lo que se indica con el dígito «2» en la expresión escaneada.

2. Configure la etiqueta de directiva `pre-ldap-epa-label`, que aloja la directiva para el análisis de la EPA.

```
add authentication policylabel pre-ldap-epa-label -loginSchema LSCHEMA_INT
<!--NeedCopy-->
```

   > **Nota:**
   >
   > LSCHEMA_INT es un esquema incorporado sin esquema (noschema), lo que significa que no se presenta ninguna página web adicional al usuario en este paso.

3. Asocie la directiva configurada en el paso 1 con la etiqueta de directiva configurada en el paso 2. Esto completa el mecanismo de autenticación.

```
bind authentication policylabel pre-ldap-epa-label -policyName pre-ldap-epa-pol -priority 100 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. Configure una acción y una directiva de LDAP.

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60 -ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net -ldapBindDnPassword 1.cloud -ldapLoginName samAccountName -groupAttrName memberOf -subAttributeName CN -passwdChange ENABLED

add authentication Policy ldap-pol -rule true -action ldap-act
<!--NeedCopy-->
```

5. Cree un esquema de inicio de sesión con el SSO activado.

```
add authentication loginSchema ldap-schema -authenticationSchema "/nsconfig/loginschema/LoginSchema/SingleAuth.xml" -SSOCredentials Yes
```



```
<!--NeedCopy-->
```

6. Configure la etiqueta de la directiva `ldap-pol-label`, que aloja la directiva para la autenticación LDAP.

```
add authentication policylabel ldap-pol-label -loginSchema ldap-schema
<!--NeedCopy-->
```

7. Enlaza el esquema de inicio de sesión configurado en el paso 5 a la etiqueta de directiva configurada en el paso 6.

```
bind authentication policylabel ldap-pol-label -policyName ldap-pol -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

8. Cree una acción para realizar un escaneo de la EPA después de la autenticación de LDAP y asócielo a una directiva de escaneo de la EPA.

```
add authentication epaAction post-ldap-epa-action -csecexpr "sys.client_expr ("proc_2_chrome")"

add authentication Policy post-ldap-epa-pol -rule true -action post-ldap-epa-action

add authentication policylabel post-ldap-epa-label -loginSchema LSCHEMA_INT

bind authentication policylabel post-ldap-epa-label -policyName post-ldap-epa-pol -priority 100 -gotoPriorityExpression
<!--NeedCopy-->
```

9. Al juntarlo todo, asocie la directiva `pre-ldap-epa-pol` al servidor virtual de autenticación y, el siguiente paso, apunte a la etiqueta de la directiva `ldap-pol-label` para realizar un análisis de la EPA.

```
bind authentication vserver user.auth.test -policy pre-ldap-epa-pol -priority 100 -nextFactor ldap-pol-label -gotoPriorityExpression NEXT

bind authentication policylabel ldap-pol-label -policyName ldap-pol -priority 100 -gotoPriorityExpression NEXT -nextFactor post-ldap-epa-label
<!--NeedCopy-->
```

Nota:

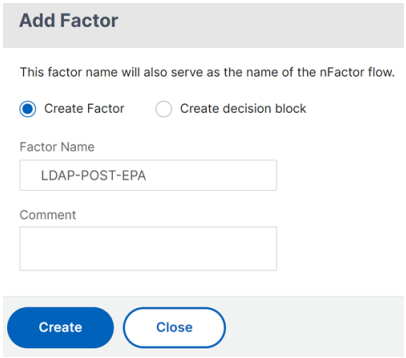
- En EPA periódico configurado como factores múltiples, se considera el factor más reciente con una configuración de EPA periódica.

> - Los escaneos periódicos solo se pueden ejecutar con el complemento de la EPA y no en el explorador.
> - En el primer ejemplo, la EPA es el primer factor en el que el escaneo busca el proceso «Firefox».
> - Si el escaneo de EPA se realiza correctamente, se inicie la autenticación LDAP, seguida del siguiente escaneo de EPA, que busca el proceso "Chrome".
> - Cuando se configuran varias exploraciones periódicas como factores diferentes, la última exploración tiene prioridad. En este caso, el complemento de la EPA busca el proceso «Chrome» cada 2 minutos después de iniciar sesión correctamente.

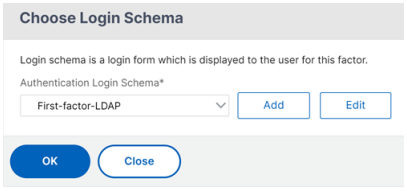
En la GUI (con nFactor Visualizer)

Puede configurar el escaneo de EPA avanzado como factor mediante el visualizador nFactor de la GUI. En el siguiente ejemplo, hemos utilizado LDAP como primer factor y EPA como el siguiente factor.

1. Cree un primer factor para el flujo nFactor.
   - Vaya a **Seguridad > Tráfico de aplicaciones AAA > Visualizador de nFactor > Flujos de nFactor** y haga clic en **Agregar**.
   - Haga clic en **+** para agregar el flujo nFactor.
   - Agregue un factor y haga clic en **Crear**.

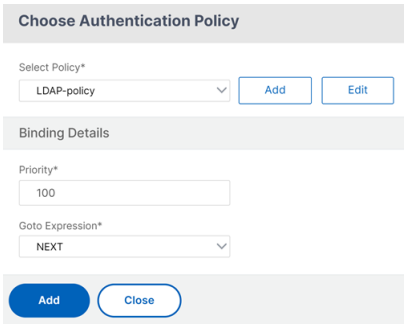


2. Cree un esquema de inicio de sesión y una directiva para el primer factor.
   - En el mosaico del primer factor, haga clic en **Agregar esquema** para agregar un esquema de inicio de sesión. Puede seleccionar un esquema de inicio de sesión de autenticación existente de la lista desplegable o crear un esquema de inicio de sesión.
   - Para crear un esquema de inicio de sesión de autenticación, haga clic en **Agregar**. Para obtener información detallada sobre el esquema de inicio de sesión de autenticación, consulte Configurar la autenticación nFactor.



- Haga clic en **Agregar directiva** para agregar la directiva LDAP. Si la directiva LDAP ya está creada, puede seleccionarla. Haga clic en **Agregar**.

  > **Nota:**
  >
  > Si no se ha creado una directiva de LDAP, puede crearla. Haga clic en el botón **Agregar** situado junto a la lista desplegable **Seleccione una directiva**. En el campo **Acción**, seleccione LDAP. Para obtener más información sobre cómo agregar un servidor LDAP de autenticación, consulte `https://support.citrix.com/article/CTX123782`.

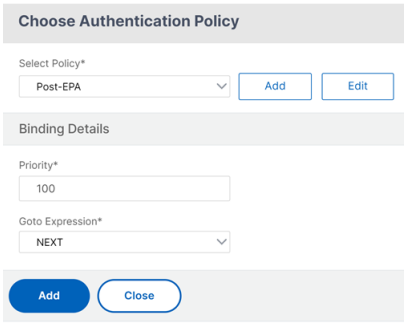


3. Cree un factor siguiente y conéctelo con el primer factor.

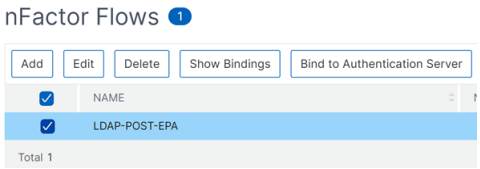
   - Haga clic en el icono **+** de color verde o rojo para agregar EPA como el siguiente factor.
   - Cree el siguiente factor en la página **Siguiente factor para conectar**.
   - Deje la sección **Agregar esquema** vacía para que no se aplique ningún esquema de forma predeterminada a este factor.

4. Agregue una directiva para el siguiente factor.

   - Haga clic en **Agregar directiva** para agregar la directiva y la acción de EPA posteriores a la autenticación.
   - Puede elegir entre una lista de directivas existente o crear una directiva. Para elegir entre las directivas existentes, seleccione una directiva de la lista desplegable **Seleccione una directiva**, proporcione los detalles vinculantes y haga clic en **Agregar**.
   - Para crear una directiva, haga clic en el botón **Agregar** situado junto a la lista desplegable **Seleccione una directiva**.



5. Una vez completado el flujo de nFactor, haga clic en **Listo**.
6. Vincule el flujo de nFactor con un servidor de autenticación.
   - Vaya a **Seguridad AAA: Tráfico de aplicaciones > nFactor Visualizer > Flujos de nFactor**.
   - Seleccione el nFactor y haga clic en **Vincular al servidor de autenticación**.



Referencias

- Conceptos, entidades y terminología de nFactor
- Cómo configurar la autenticación LDAP en NetScaler Gateway
- Autenticación LDAP
- Análisis avanzado de endpoints

Tipos de clasificación de análisis EPA en el cliente Windows

March 27, 2024

> **Importante:**
>
> El objetivo de Endpoint Analysis es analizar el dispositivo del usuario según criterios de cumplimiento predeterminados y no hace cumplir ni validar la seguridad de los dispositivos de los usuarios finales. Se recomienda utilizar sistemas de seguridad de dispositivos de punto final para proteger los dispositivos de los ataques de los administradores locales.

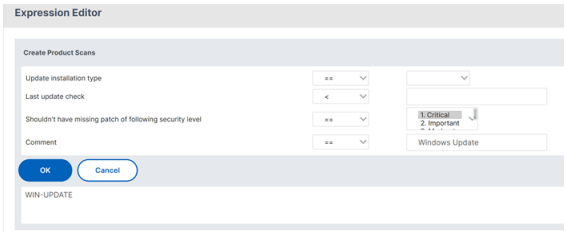
Los siguientes tipos de clasificación nuevos se agregan al análisis EPA en busca de parches que falten. El análisis EPA falla si el cliente tiene alguno de los siguientes parches que faltan.

- Aplicación
- Conectores
- CriticalUpdates
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Guidance
- SecurityUpdates
- ServicePacks
- Herramientas
- UpdateRollups
- Actualizaciones

> **Notas:**
>
> - Anteriormente, los análisis de EPA para detectar los parches faltantes se realizaban en los niveles de gravedad: crítico, importante, moderado y bajo en el cliente de Windows.
> - Si utiliza Citrix Secure Access para Windows 23.8.1.1 y versiones posteriores, el análisis `CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` se limita a las máquinas cliente que tengan habilitadas las actualizaciones automáticas. Si las actualizaciones automáticas están inhabilitadas, este análisis arroja un resultado diferente.

Configurar los tipos de clasificación de análisis EPA mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > Autenticación previa**.
2. Cree una directiva de autenticación previa o modifique una directiva existente.
3. Haga clic en el enlace **Editor de EPA OPSWAT**.
4. En el Editor de expresiones, seleccione **Windows > Windows Update**.
5. En **No debe faltar el parche del siguiente tipo de clasificación de actualizaciones de Windows**, seleccione el tipo de clasificación para los parches que faltan.
6. Haga clic en **Aceptar**.



Los clientes pueden actualizar a la versión 4.3.2744.0s de OPSWAT para usar estas opciones.

Referencias

- Para obtener más información sobre los GUID de clasificación de los servicios de actualización de Windows Server, consulte https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85).
- Para obtener una descripción de la terminología de actualizaciones de software de Microsoft, consulte https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates.

Análisis avanzado de endpoints

March 27, 2024

El análisis avanzado de terminales (EPA) se utiliza para analizar los dispositivos de los usuarios en busca de los requisitos de seguridad de terminales configurados en NetScaler Gateway. Si un dispositivo de usuario intenta acceder a NetScaler Gateway, se escanea en busca de información de seguridad, como el sistema operativo, el antivirus, las versiones del explorador web, etc., antes de que un administrador pueda conceder el acceso a NetScaler Gateway.

El análisis EPA avanzado es un análisis basado en directivas que puede configurar en NetScaler Gateway para las sesiones de autenticación. La directiva realiza una comprobación del registro en un dispositivo de usuario y, en función de la evaluación, permite o deniega el acceso a la red NetScaler. Para obtener más información sobre los requisitos del sistema cliente Citrix EPA, consulte Requisitos de Endpoint Analysis.

Puede configurar el escaneo de EPA avanzado mediante la GUI o la CLI.

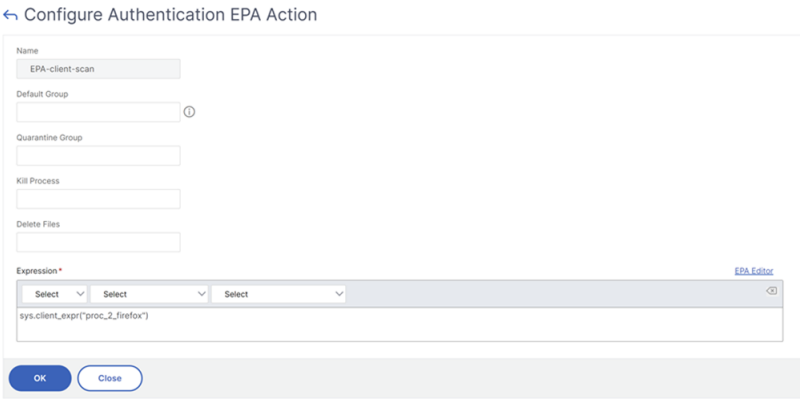
En la GUI

1. Cree una acción de EPA.

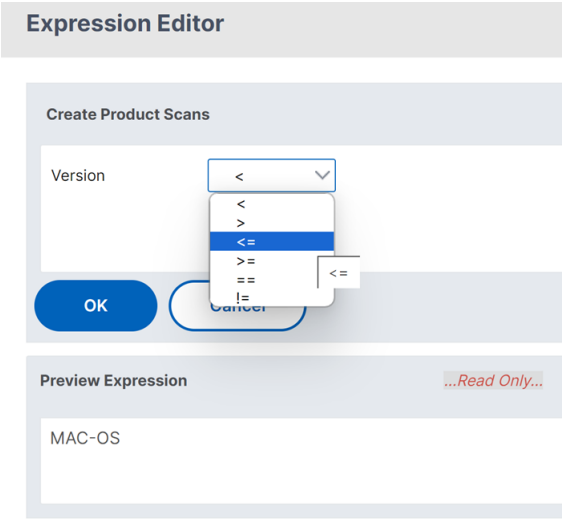
   Vaya a **Seguridad > AAA: tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Acciones > EPA** y haga clic en **Agregar**. En la página **Crear acción EPA de autenticación**, actualice la siguiente información y haga clic en **Crear**.

   - Nombre: Nombre de la acción de EPA.
   - Grupo predeterminado: El grupo predeterminado que se elige cuando la comprobación de EPA se realiza correctamente.
   - Grupo de cuarentena: El grupo de cuarentena que se elige cuando falla la comprobación de EPA.

- Detener proceso: Cadena que especifica el nombre de un proceso que el plug-in de EPA debe detener. Los procesos múltiples deben estar separados por comas.
- Eliminar archivos: Cadena que especifica las rutas y los nombres de los archivos que eliminará el plug-in de EPA. Los archivos múltiples deben estar separados por comas.
- Expresión: Consulte la Referencia de expresiones de directivas de Advanced Endpoint Analysis para conocer el formato de expresión de EPA.



- Editor de la EPA: seleccione los operadores para el escaneo de la versión del producto.



Nota:

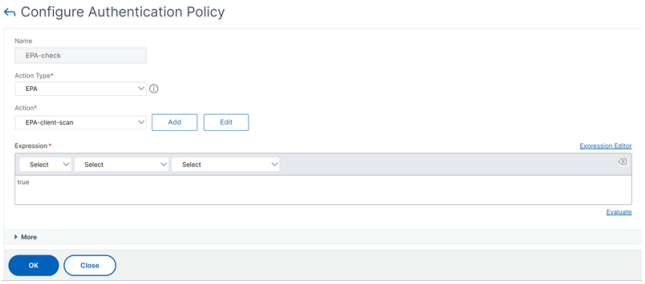
El cliente Citrix EPA para macOS 24.2.1.5/El cliente Citrix Secure Access para macOS 24.02.1 y versiones posteriores admiten los operadores EPA >, <, >=, <=, == y != en el editor EPA. Además, la opción **Mac OS** ahora está disponible como una opción independiente en el editor de la EPA (**Mac > Mac OS**). Anteriormente, el escaneo de la versión del producto macOS tenía que realizarse en **Common > Operating System > macOS** utilizando solo los operadores == y !=. Asegúrese de utilizar NetScaler Gateway 14.1-12.x o una versión posterior para aprovechar esta funcionalidad.

> Puedes escanear la versión del producto de tus dispositivos macOS en **Mac > Mac OS** con estos operadores. Por ejemplo, para permitir las versiones del sistema operativo de la 12.4 a la 13.0, excepto la 12.8, configure la expresión `sys.client_expr("sys_0_MAC-OS_version_>=_12.4")&&sys.client_expr("sys_0_MAC-OS_version_<=_13.0")&&sys.client_expr("sys_0_MAC-OS_version_!=_12.8")` en el editor de la EPA.

2. Cree la directiva de EPA correspondiente.

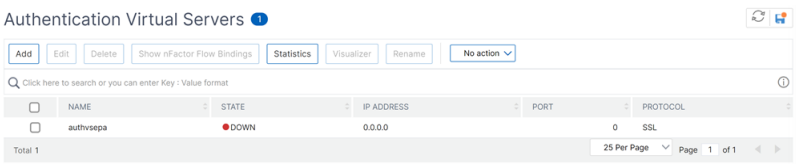
   Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Directivas > Autenticación > Directivas avanzadas > Directivas** y haga clic en **Agregar**. En la página **Crear directiva de autenticación**, actualice la siguiente información y haga clic en **Crear**.

   - Nombre: Nombre de la directiva avanzada de EPA.
   - Tipo de acción: Tipo de acción de autenticación.
   - Acción: Nombre de la acción de autenticación que se realizará si la directiva coincide.
   - Expresión: Consulte la Referencia de expresiones de directivas de Advanced Endpoint Analysis para conocer el formato de expresión de EPA.
   - Acción de registro: nombre de la acción de registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva. La longitud máxima permitida es de 127 caracteres.

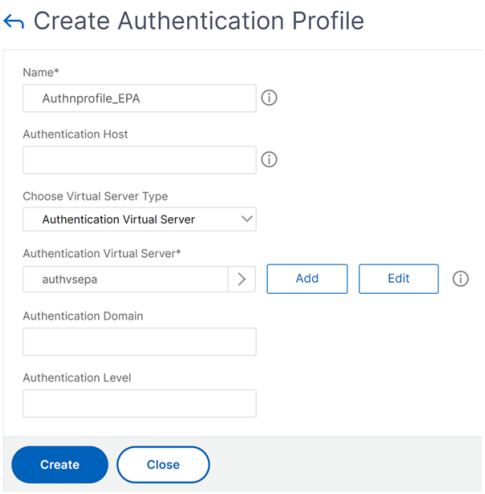


3. Configure un servidor virtual de autenticación y un perfil de autenticación.

   - Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Servidores virtuales de autenticación** y haga clic en **Agregar**.

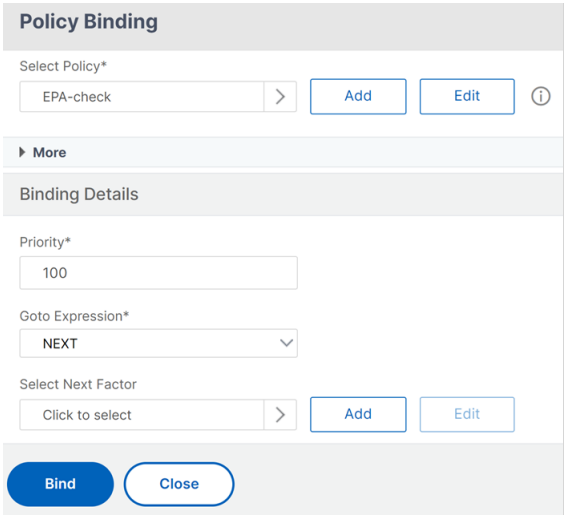


   - Vaya a **Seguridad > AAA - Tráfico de aplicaciones > Perfil de autenticación** y haga clic en **Crear**.



4. Vincule la directiva de EPA avanzada al servidor virtual de autenticación.

   - Vaya a **Seguridad > AAA —Tráfico de aplicaciones > Servidores virtuales de autenticación** y seleccione el servidor virtual de autenticación.
   - Seleccione la directiva en la sección **Directivas de autenticación avanzadas**.
   - Haga clic en **Vincular** en la sección **Vinculación de directivas**.



5. Vincule la directiva de EPA al flujo de nFactor.

   Para obtener más información sobre cómo agregar una directiva de EPA avanzada como factor al flujo de nFactor, consulte Escaneo de EPA como factor en la autenticación de nFactor.

En la CLI

1. Cree una acción para realizar el escaneo de EPA.

```
1 add authentication epaAction EPA-client-scan -csecexpr "sys.
    client_expr ("proc_2_firefox")"
```



```
<!--NeedCopy-->
```

La expresión anterior analiza si el proceso 'Firefox'se está ejecutando. El plug-in de la EPA comprueba la existencia del proceso cada 2 minutos, lo que significa el dígito "2"en la expresión de escaneo.

2. Asocie la acción de EPA a una directiva avanzada de EPA.

```
add authentication Policy EPA-check -rule true -action EPA-client-scan
<!--NeedCopy-->
```

3. Configure un servidor virtual de autenticación y un perfil de autenticación.

```
add authentication vserver authnvsepa ssl -ip address 10.104.130.129 -port 443
<!--NeedCopy-->
```

```
add Authnprofile_EPA -authnVsName authnvsepa
<!--NeedCopy-->
```

4. Vincule la directiva de EPA avanzada al servidor virtual de autenticación.

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
<!--NeedCopy-->
```

Actualización de bibliotecas EPA

Para utilizar la GUI de NetScaler para actualizar las bibliotecas EPA:

1. Vaya a**Configuración > NetScaler Gateway > Actualizar componentes de cliente**.
2. En **Actualizar componentes de cliente,** haga clic en el enlace **Actualizar bibliotecas de EPA**.
3. Elija el archivo necesario y haga clic en **Actualizar**.

> **Importante:**
>
> - En una alta disponibilidad de NetScaler Gateway, las bibliotecas EPA deben actualizarse tanto en el nodo principal como en el secundario.
> - En una configuración de clústeres de NetScaler Gateway, las bibliotecas EPA deben actualizarse en todos los nodos del clúster.

Para obtener la lista de aplicaciones compatibles con Windows y MAC por OPSWAT para exploraciones de NetScaler, consulte https://support.citrix.com/article/CTX234466.

Solución de problemas de análisis avanzados de Endpoint Analysis

Para ayudar a solucionar problemas de análisis de análisis avanzado de endpoints, los plug-ins cliente escriben información de registro en un archivo de los sistemas de endpoints cliente. Estos archivos de registro se encuentran en los siguientes directorios, según el sistema operativo del usuario.

Windows Vista, Windows 7, Windows 8, Windows 8.1 y Windows 10:

C:\Usuarios\<nombre_de_usuario>\AppData\Local\Citrix\AGEE\nsepa.txt

Windows XP:

C:\Documents and Settings\Todos los usuarios\Datos de aplicaciones\Citrix\AGEE\nsepa.txt

Sistemas Mac OS X:

~/Biblioteca/Application Support/Citrix/EPAPlugin/epaplugin.log

(Donde el símbolo ~ indica la ruta del directorio principal del usuario de macOS correspondiente).
(Donde el símbolo ~ indica la ruta del directorio principal del usuario de macOS correspondiente).

Ubuntu:

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

Referencia de expresiones de directivas de análisis avanzado de endpoints

January 26, 2024

En este tema se describe el formato y la construcción de las expresiones Advanced Endpoint Analysis. La utilidad de configuración de NetScaler Gateway crea automáticamente los elementos de expresión contenidos aquí y no requiere configuración manual.

Formato de expresión

Una expresión de análisis avanzado de puntos finales tiene el siguiente formato:

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _...)
```

Donde:

El tipo de escaneo es el tipo de aplicación que se analiza.

Product-ID es la identificación del producto para la aplicación analizada.

El nombre del método es el atributo del producto o del sistema que se está analizando.

El comparador de métodos es el comparador elegido para el análisis.

method-param es el valor o valores de atributo que se analizan.

Ejemplo:

client.application(ANTIVIR_2600*RTP*==_TRUE)

> **Nota:**
>
> Para los tipos de exploración ajenos a aplicaciones, el prefijo de expresión es CLIENT.SYSTEM en lugar de CLIENT.APPLICATION.

Cadenas de expresión

Cada uno de los tipos de análisis admitidos en Advanced Endpoint Analysis utiliza un identificador único en las expresiones. En la tabla siguiente se enumeran las cadenas de cada tipo de análisis.

Tipo de escaneo	Cadena de expresión tipo escaneo
Antiphishing	ANTIPHI
Antispyware	ANTISPY
Antivirus	ANTIVIR
Cliente de backup	BACKUP
Control de acceso a dispositivos	DEV-CONT
Prevención de pérdida de datos	DATA-PREV
Uso compartido de escritorio	DESK-SHARE
Firewall	FIREWALL
Agente de salud	HEALTH
Cifrado de disco duro	HD-ENC
Mensajería instantánea	IM
Explorador web	BROWSER
P2P	P2P
Administración de parches	PATCH
Filtrado de URL	URL-FILT

Tipo de escaneo	Cadena de expresión tipo escaneo
Dirección MAC	MAC
Comprobación de dominio	DOMAIN
Análisis numérico del registro	REG-NUM

> **Nota:**
>
> Para los análisis específicos de macOS X, las expresiones incluyen el prefijo MAC- antes del tipo de método. Por lo tanto, para los análisis antivirus y antiphishing, los métodos son MAC-ANTIVIR y MAC-ANTIPHI respectivamente.
>
> Por ejemplo:
>
> client.application(MAC-ANTIVIR_2600*RTP*==_TRUE)

Métodos de exploración de aplicaciones

Al configurar expresiones de análisis avanzado de endpoints, se utilizan métodos para definir los parámetros de los análisis de endpoints. Estos métodos incluyen un nombre de método, un comparador y un valor. En las tablas siguientes se enumeran los métodos disponibles para su uso en expresiones.

Métodos de exploración comunes:

Los métodos siguientes se utilizan para varios tipos de análisis de aplicaciones.

Método	Descripción	Comparador	Valores posibles
VERSIÓN*	Especifica la versión de la aplicación.	<, <=, >, >=, !=, ==	Cadena de versión
AUTHENTIC**	Comprueba si la aplicación es auténtica o no.	==	TRUE
HABILITADO	Compruebe si la aplicación está habilitada.	==	TRUE
EJECUTÁNDOSE	Compruebe si la aplicación se está ejecutando.	==	TRUE

Método	Descripción	Comparador	Valores posibles
COMENTARIO	Campo de comentario (ignorado por el análisis). Delineado por [] dentro de las expresiones.	==	Cualquier texto

* La cadena VERSION puede especificar una cadena decimal de hasta cuatro valores, como 1.2.3.4.

** Una comprobación AUTHENTIC verifica la autenticidad de los archivos binarios de la aplicación.

> **Nota:**
>
> Puede seleccionar una versión genérica para los tipos de análisis de aplicaciones. Cuando se seleccionan escaneos genéricos, el identificador del producto es 0.

Gateway ofrece una opción para configurar los análisis genéricos para cada tipo de software. Mediante el análisis genérico, un administrador puede escanear el equipo cliente sin restringir la comprobación del análisis a ningún producto en particular.

En el caso de los análisis genéricos, los métodos de exploración solo funcionan si el producto instalado en el sistema del usuario admite ese método de exploración. Para saber qué productos admiten un método de escaneo determinado, póngase en contacto con el soporte de NetScaler.

Métodos de escaneo únicos:

Los métodos siguientes son exclusivos de los tipos de análisis especificados.

Método	Descripción	Comparador	Valores posibles
ENABLED-FOR	Compruebe si el software antiphishing está habilitado para la aplicación seleccionada.	`allof`, `anyof`, `noneof`	**Para Windows**: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari. **Para Mac:** Safari, Mozilla Firefox, Google, Chrome, Opera

Tabla 2. Antispyware y antivirus

Método	Descripción	Comparador	Valores posibles
RTP	Compruebe si la protección en tiempo real está activada o no.	==	TRUE
SCAN-TIME	Cuántos **minutos** han transcurrido desde que se realizó un análisis completo del sistema.	<, <=, >, >=, !=, ==	Cualquier número positivo
VIRDEF-FILE-TIME	Cuántos **minutos** han transcurrido desde que se actualizó el archivo de definición de virus (es decir, número de minutos entre la marca de archivo de definición de virus y la fecha y hora actual).	<, <=, >, >=, !=, ==	Cualquier número positivo
VIRDEF-FILE-VERSION	Versión del archivo de definición.	<, <=, >, >=, !=, ==	Cadena de versión
ENGINE-VERSION	Versión motor.	<, <=, >, >=, !=, ==	Cadena de versión

Tabla 3. Cliente de reserva

Método	Descripción	Comparador	Valores posibles
LAST-BK-ACTIVITY	Cuántos **minutos** han pasado desde que se completó la última actividad de copia de seguridad.	<, <=, >, >=, !=, ==	Cualquier número positivo

Tabla 4. Prevención de pérdida de datos

Método	Descripción	Comparador	Valores posibles
HABILITADO	Compruebe si la aplicación está habilitada o no y si la protección horaria está activada o no.	==	TRUE

Tabla 5. Agente de chequeo de estado

Método	Descripción	Comparador	Valores posibles
SYSTEM-COMPL	Compruebe si el sistema cumple los requisitos.	==	TRUE

Tabla 6. Cifrado de disco duro

Método	Descripción	Comparador	Valores posibles
ENC-PATH	PATH para comprobar el estado del cifrado.	SIN OPERADOR	Cualquier texto
ENC-TYPE	Compruebe si el tipo de cifrado de la ruta especificada.	`allof`, `anyof`, `noneof`	**Lista con las siguientes opciones**: UNENCRYPTED, PARTIAL, ENCRYPTED, VIRTUAL, SUSPENDED, PENDING

Tabla 7. Explorador web

Método	Descripción	Comparador	Valores posibles
PREDETERMINADO	Compruebe si está configurado como explorador predeterminado.	==	TRUE

Tabla 8. Gestión de parches </caption>

Método	Descripción	Comparador	Valores posibles
—	—	—	—
SCAN-TIME	Cuántos minutos han transcurrido desde que se realizó la última exploración del parche.	<, <=, >, >=, !=, ==	Cualquier número positivo
MISSED-PATCH	En el sistema cliente no faltan parches de este tipo.	`anyof`, `noneof`	CUALQUIER preseleccionado (parches preseleccionados en el servidor de Patch Manager)
NON

Cuadro 9. Dirección MAC

Método	Descripción	Comparador	Valores posibles
ADDR	Compruebe si las direcciones MAC del equipo cliente están o no en la lista especificada.	`anyof`, `noneof`	Lista modificable

Cuadro 10. Pertenencia a

Método	Descripción	Comparador	Valores posibles
SUFFIX	Compruebe si el equipo cliente existe o no existe en la lista dada.	`anyof`, `noneof`	Lista modificable

Cuadro 11. Entrada de registro numérico

Método	Descripción	Comparador	Valores posibles
PATH	Ruta de acceso para la comprobación del registro. En el formato: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate. No es necesario que se escapen los caracteres especiales. Todas las claves raíz del registro: HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG	SIN OPERADOR	Cualquier texto

Método	Descripción	Comparador	Valores posibles
REDIR-64	Siga la redirección de 64 bits. Si se establece en TRUE, se sigue la redirección WOW (es decir, la ruta de registro se comprueba en sistemas de 32 bits, pero la ruta redirigida de WOW se comprueba para los sistemas de 64 bits). Si no se establece, no se sigue la redirección WOW (es decir, se comprueba la misma ruta de registro para los sistemas de 32 bits y 64 bits). Para las entradas de registro que no se redirigen, esta configuración no tiene efecto. Consulte el siguiente artículo para obtener una lista de claves de registro que se redireccionan en sistemas de 64 bits: http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx	==	TRUE

Método	Descripción	Comparador	Valores posibles
VALOR	Valor esperado para la ruta anterior. Este análisis solo funciona para los tipos de registro de REG_DWORD y REG_QWORD.	<, <=, >, >=, !=, ==	Cualquier número

Análisis de EPA en busca de direcciones MAC

March 27, 2024

A partir de la versión 13.0-88.x de NetScaler, puede configurar las configuraciones de análisis de EPA para las direcciones MAC permitidas o específicas. NetScaler utiliza expresiones de directivas y conjuntos de patrones para especificar la lista de direcciones MAC.

Antes de la versión 13.0-88.x de NetScaler, la lista de todas las direcciones MAC permitidas debía especificarse como parte de una expresión de EPA. Si los clientes tenían una lista enorme de direcciones MAC permitidas, resultaba engorroso agregar todas las direcciones MAC en una sola expresión. Además, había una limitación en la cantidad de direcciones MAC que se agregaban en una sola expresión.

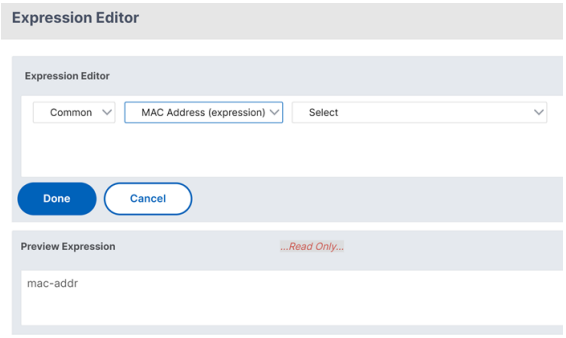
Por ejemplo,

```
1 add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome") || sys.
    client_expr("proc_0_firefox") && sys.client_expr("
    sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT: MAC Address]
    ")/
2 <!--NeedCopy-->
```

Configurar el análisis de EPA de direcciones MAC mediante la interfaz gráfica de usuario

Ahora, la opción **Direcciones MAC (expresión)** que estaba disponible anteriormente en la categoría de análisis **Windows** está disponible en la categoría de análisis **Común** de la GUI de NetScaler. Esta opción permite a los usuarios configurar un análisis de EPA para obtener una lista de direcciones MAC específicas o permitidas.

> **Nota:**
>
> El cliente Citrix Secure Access 22.10.1 y las versiones posteriores admiten este método en el que NetScaler gestiona las configuraciones de escaneo EPA en la GUI.



1. Configure un conjunto de patrones. Para obtener más información, consulte Configuración de un conjunto de patrones.
2. Cree una expresión de directiva correspondiente para cada conjunto de patrones.

   Al configurar la expresión, en el Editor de expresiones, seleccione **AAA > LOGIN > CLIENT_MAC_ADDR > EQUAL_ANY(cadena) > Conjunto de patrones**.

   Para obtener más información sobre la configuración de una expresión avanzada, consulte Configurar expresiones de directiva avanzadas en una directiva.
3. Cree un análisis de EPA para la expresión configurada en los pasos anteriores. Para obtener más información, consulte Análisis avanzados de endpoints.

Configurar el análisis de EPA de direcciones MAC mediante la CLI

1. Almacene las direcciones MAC dentro de conjuntos de patrones.

   En la línea de comandos, escriba;

   ```
   add policy patset <name> [-comment <string>]
   <!--NeedCopy-->
   ```

   Example:

   “‘

   add policy patset patset1
   bind policy patset patset1 1A-C8-9C-83-BO-F7
   bind policy patset1 02-50-F2-0A-77-7C…y así sucesivamente hasta 3K entradas.
   add policy patset patset2
   bind policy patset2 patset2 1A-2B-3C-4D-5E-6A

bind policy patset2 1A-2B-3C-4D-5E-6B…y así sucesivamente hasta 3K entradas.
‘‘‘

2. Cree una expresión de directiva correspondiente para cada conjunto de patrones mediante aaa.login.client_mac_addr.equals_any ()

   En la línea de comandos, escriba;

```
Add policy expression <name> <value> [-comment <string>] [-
    clientSecurityMessage <string>]
```

   Ejemplo:

```
add policy expression exp1 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
    patset1")
add policy expression exp2 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
    patset2")
```

3. Cree escaneos de EPA mediante las expresiones de directivas

   En la línea de comandos, escriba;

```
add authentication epaAction <name>  -csecexpr <expression>
```

   Ejemplo:

```
add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")  ||
    sys.client_expr("mac-addr_0_exp1") || sys.client_expr("mac-
    addr_0_exp2") || sys.client_expr("proc_0_firefox")/
```

   Configurar una directiva de preautenticación,

```
add authentication Policy epapol -rule true -action epa
```

   Vincular la directiva de preautenticación,

```
bind authentication vserver <name> -policy epapol -priority 10 -
    gotoPriorityExpression NEXT
```

Puntos que tener en cuenta

- La configuración de un escaneo EPA para obtener una lista permitida de direcciones MAC solo se aplica a los flujos de autenticación de nFactor.
- Se recomienda almacenar no más de 3000 entradas en un conjunto de patrones.
- Las direcciones MAC deben configurarse en el formato 1A-2B-3C-4D-5E-6F.
- El formato de la exploración de EPA es `mac-addr_0_<policy-expression-name>`. En este formato, `mac-addr_0_` es un valor estático y debe introducir el nombre de la expresión de directiva después de `mac-addr_0_`.

- Las exploraciones de EPA se pueden separar adecuadamente con los símbolos (`||`, `&&`).
- Para agregar muchas direcciones MAC a un conjunto de patrones, puede utilizar la importación de conjuntos de patrones basados en archivos. Se recomienda almacenar un máximo de 3000 entradas/conjunto de patrones para un rendimiento óptimo.
- Si las direcciones MAC están presentes dentro de un archivo, puede crear un conjunto de patrones mediante la importación de conjuntos de patrones basados en archivos y especificando el delimitador apropiado durante la importación.

Referencias

- Configure un conjunto de patrones.
- Cree un conjunto de patrones mediante la importación basada en archivos.
  “‘

Administrar sesiones de usuario

January 26, 2024

Puede administrar las sesiones de usuario en la GUI de NetScaler desde el cuadro de diálogo **Sesiones de usuarios activos**. Este cuadro de diálogo muestra una lista de las sesiones de usuario activas en NetScaler Gateway. Puede ver las sesiones de usuario final o grupo mediante el nombre de usuario, el nombre del grupo o la dirección IP. También puede ver las sesiones activas en este cuadro de diálogo. La información de la sesión incluye:

- Nombre de usuario
- Dirección IP del dispositivo del usuario
- Número de puerto del dispositivo de usuario
- Dirección IP del servidor virtual
- Número de puerto del servidor virtual
- Dirección IP de intranet asignada al usuario

Administrar las sesiones de usuario mediante la interfaz gráfica de usuario

Para ver las sesiones de usuario

1. En el panel de navegación de la GUI de NetScaler, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. En **Sesiones de usuario activas**, seleccione uno de los siguientes tipos.

- **Usuarios activos**
- **Grupos activos**
- **IP de intranet**: cuando selecciona IP de intranet, debe introducir la dirección IP de la intranet y la máscara de subred.

4. Haga clic en **Continuar**.

Para actualizar la lista de sesiones

Puede recuperar información actualizada sobre las sesiones en NetScaler Gateway.

1. En el panel de navegación de la GUI de NetScaler, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. Haga clic en **Actualizar**.

Para sesiones de usuario final o grupo o una sesión que tiene una dirección IP de intranet específica

Puede terminar las sesiones de usuario y grupo. También puede finalizar una sesión que tenga una dirección IP de intranet y una máscara de subred específicas.

1. En el panel de navegación de la GUI de NetScaler, haga clic en **NetScaler Gateway**.
2. En el panel de detalles, en Supervisar conexiones, haga clic en **Sesiones de usuario activas**.
3. En Sesiones, seleccione un usuario, grupo o sesión que tenga una dirección IP de intranet específica y, a continuación, haga clic en **Finalizar**.

Administrar las sesiones de usuario mediante la CLI

Puede utilizar los siguientes comandos de CLI para ver las sesiones de usuario, usuario final o grupo.

- `show aaa session`- Muestra todas las conexiones VPN o de autenticación, autorización y auditoría de NetScaler enlazadas al usuario, grupo, dirección IP o intervalo IP especificados.
- `show vpn icaConnection` - Muestra todas las conexiones activas que utilizan el proxy ICA.
- `show system session`: Muestra información sobre todas las sesiones actuales del sistema o sobre la sesión especificada.

Always On

March 27, 2024

La función Always On de NetScaler Gateway garantiza que los usuarios estén siempre conectados a la red empresarial. Esta conectividad VPN persistente se consigue mediante el establecimiento automático de un túnel VPN.

> **Nota**
>
> La función Always On admite portales cautivos para NetScaler 12.0 compilación 51.24 y versiones posteriores.

Cuándo usar Always On

Utilice Always On cuando necesite proporcionar conectividad VPN fluida basada en la ubicación del usuario y tenga que impedir el acceso a la red de un usuario que no está conectado a una VPN.

En los siguientes casos se ilustra el uso de Always On.

- Un empleado inicia el portátil fuera de la red empresarial y necesita ayuda para establecer la conectividad VPN.
  Solución: Cuando el portátil se inicia fuera de la red empresarial, Always On establece sin problemas un túnel y proporciona conectividad VPN.
- Un empleado que utiliza conectividad VPN se traslada a la red empresarial. El empleado se cambia a una red empresarial pero permanece conectado al túnel VPN, lo cual no es un estado deseable.
  Solución: Cuando el empleado se traslada a la red empresarial, Always On derriba el túnel VPN y cambia sin problemas al empleado a la red empresarial.
- Un empleado se traslada fuera de la red empresarial y cierra el portátil (no lo apaga). El empleado necesita ayuda para establecer la conectividad VPN al reanudar el trabajo en el portátil.
  Solución: Cuando el empleado se mueve fuera de la red empresarial, Always On establece sin problemas un túnel y proporciona conectividad VPN.
- Una empresa quiere regular el acceso a la red que se proporciona a sus usuarios cuando no están conectados a un túnel VPN.
  Solución: Según la configuración, Always On restringe el acceso, lo que permite a los usuarios acceder únicamente a la red de puerta de enlace.

Comprensión del marco Always On

Always On conecta automáticamente a un usuario a un túnel VPN que el cliente ha establecido previamente. La primera vez que el usuario necesita un túnel VPN, debe conectarse a la URL de NetScaler Gateway y establecer el túnel. Una vez descargada la configuración Always On en el cliente, esta configuración impulsa el establecimiento posterior del túnel.

El ejecutable del cliente Citrix Secure Access siempre se ejecuta en el equipo cliente. Cuando el usuario inicia sesión o la red cambia, el cliente Citrix Secure Access determina si el portátil del usuario está en la red empresarial. Según la ubicación y la configuración, el cliente Citrix Secure Access establece un túnel o derriba un túnel existente.

El establecimiento del túnel se inicia solo después de que el usuario inicie sesión en el equipo. El cliente Citrix Secure Access utiliza las credenciales del equipo cliente para autenticarse con el servidor de puerta de enlace e intenta establecer un túnel.

Restablecimiento automático de un túnel

El restablecimiento automático de un túnel se activa cuando NetScaler Gateway derriba un túnel VPN.

> **Nota**
>
> Cuando se produce un error en el análisis de dispositivos de punto final, el cliente de NetScaler Gateway no vuelve a intentar establecer el túnel, sino que muestra un mensaje de error. Si se produce un error de autenticación, el cliente de NetScaler Gateway solicita credenciales al usuario.

Métodos de autenticación de usuarios compatibles para establecer túneles sin problemas

Los métodos de autenticación de usuarios compatibles son los siguientes:

- Nombre de usuario y contraseña de AD: si se utilizan el nombre de usuario y la contraseña de Windows para la autenticación, el cliente Citrix Secure Access establece el túnel sin problemas mediante estas credenciales.
- Certificado de usuario: si se utiliza un certificado de usuario para la autenticación y solo hay un certificado en la máquina cliente, el cliente Citrix Secure Access establece un túnel sin problemas mediante este certificado. Si hay varios certificados de cliente instalados, el túnel se establece después de que el usuario haya seleccionado el certificado preferido. El cliente Citrix Secure Access usa este certificado preferido para túneles posteriores.

  Si las tarjetas inteligentes comparten un certificado de usuario, no se puede lograr el inicio de sesión automático si los certificados se instalan de forma dinámica en el almacén en comparación con los certificados presentes en el almacén.
- Certificado de usuario y nombre de usuario + contraseña de AD: Este método de autenticación es la combinación de métodos de autenticación descritos anteriormente.

> **Nota**
>
> Se admiten todos los demás mecanismos de autenticación, pero el establecimiento del túnel no

> es transparente para ningún otro método de autenticación.

Requisitos de configuración para Always On

El administrador empresarial debe aplicar lo siguiente para los dispositivos administrados:

- El usuario no debe poder finalizar el proceso/servicio para una configuración específica
- El usuario no debe poder desinstalar el paquete para una configuración específica
- El usuario no debe poder cambiar entradas de registro específicas

> **Nota**
>
> Es posible que la función no funcione como se esperaba si el usuario tiene privilegios de administración, como en el caso de los dispositivos no administrados.

Consideraciones al habilitar la función Always On

Revise la siguiente sección antes de habilitar la función Siempre activado.

Acceso a la red principal: Cuando se establece el túnel, el tráfico hacia la red empresarial se decide en función de la configuración de túnel dividido. No se proporcionan otras configuraciones para anular este comportamiento.

Configuración de proxy del equipo cliente: la configuración del proxy del equipo cliente se ignora para conectarse al servidor de puerta de enlace.

> **Nota**
>
> La configuración de proxy del dispositivo NetScaler no se ignora. Solo se ignoran las configuraciones de proxy del equipo cliente. Los usuarios que tienen un proxy configurado en sus sistemas reciben una notificación de que el complemento VPN ha ignorado su configuración de proxy.

Configuración de Always On

Para configurar Always On, cree un perfil Always On en el dispositivo NetScaler Gateway y aplíquelo.

Para crear un perfil Always On:

1. En la GUI de NetScaler, vaya a **Configuración > NetScaler Gateway > Directivas > AlwaysOn.**
2. En la página **Perfiles de AlwaysOn**, haga clic en **Agregar**.
3. En la página **Crear perfil de AlwaysOn**, introduzca los siguientes detalles:
    - **Nombre**: El nombre de su perfil.

- **VPN basada en ubicación (nombre del registro del lado del cliente: LocationDetection): seleccione una de las siguientes opciones:
  - **Remoto** para permitir que un cliente detecte si está en la red empresarial y establezca el túnel si no en la red empresarial. El ajuste predeterminado es el control remoto.
  - **En todas partes** para permitir que un cliente omita la detección de ubicación y establezca el túnel independientemente de la ubicación del cliente
- **Control de cliente**: Seleccione una de las siguientes opciones:
  - **Denegar**para impedir que el usuario cierre la sesión y se conecte a otra puerta de enlace. Denegar es la configuración predeterminada.
  - **Permitir que** el usuario cierre sesión y se conecte a otra puerta de enlace.
- **Error de acceso a la red en VPN (nombre del registro del lado del cliente: AlwaysOn)**: Seleccione una de las siguientes opciones:
  - **Acceso completo** para permitir que el tráfico de red fluya hacia y desde el cliente cuando el túnel no está establecido. Acceso completo es la configuración predeterminada.
  - **Solo a puerta de enlace** para evitar que el tráfico de red fluya hacia o desde el cliente cuando el túnel no está establecido. Sin embargo, se permite el tráfico hacia o desde la dirección IP de la puerta de enlace.
    Nota: En el modo **Solo a puerta** de enlace, solo se desbloquean el servidor virtual, el DNS y el tráfico DHCP. Para desbloquear otros sitios web, intervalos de direcciones IP o direcciones IP, debe configurar el registro **AlwaysOnAllowlist** con una lista separada por punto y coma de FQDN, intervalos de direcciones IP o direcciones IP.
    Por ejemplo, miempresa.com,micdn.com,10.120.67.0-10.120.67.255,67.67.67.67

4. Haga clic en **Crear** para terminar de crear su perfil.

Para aplicar el perfil Always On:

1. En la interfaz de NetScaler, seleccione **Configuración > NetScaler Gateway > Configuración global**.
2. En la página Configuración global, haga clic en el vínculo **Cambiar configuración global** y, a continuación, seleccione la ficha **Experiencia del cliente**.
3. En el menú desplegable **Nombre de perfil de AlwaysOn**, seleccione el perfil recién creado y haga clic en **Aceptar**.

Nota: Se puede realizar una configuración similar en el perfil de sesión para aplicar las directivas a nivel de grupo, nivel de servidor o nivel de usuario.

Nota sobre los IIP

El túnel de nivel de máquina utiliza la autenticación basada en certificados y la sesión que se crea tiene el nombre común del certificado como nombre de usuario. Por lo tanto, si los certificados de dispositivo tienen nombres comunes únicos, las sesiones de diferentes máquinas tienen un nombre de usuario diferente y, por lo tanto, diferentes IIP. Asegúrese de generar un certificado de dispositivo con nombres únicos. Idealmente, debe utilizar los nombres de las máquinas como el nombre común del certificado del dispositivo.

Resumen de comportamiento de diferentes configuraciones para usuarios administradores y usuarios no administradores

En la tabla siguiente se resume el comportamiento de las distintas configuraciones. También detalla la posibilidad de que el usuario realice ciertas acciones, lo que puede afectar a la funcionalidad de Always On.

Error de acceso a la red en VPN	Control de clientes	Usuario no administrador	Usuario administrador
`fullaccess`	Permitir	El túnel se establece automáticamente. El usuario puede cerrar la sesión y permanecer fuera de la red. El usuario también puede apuntar a otro NetScaler Gateway.	El túnel se establece automáticamente. El usuario puede cerrar la sesión y permanecer fuera de la red empresarial. El usuario también puede apuntar a otro NetScaler Gateway.
`fullaccess`	Negar	El túnel se establece automáticamente. El usuario no puede cerrar la sesión ni apuntar a otro NetScaler Gateway.	El túnel se establece automáticamente. El usuario puede desinstalar el cliente Citrix Secure Access o pasar a otro NetScaler Gateway.

Error de acceso a la red en VPN	Control de clientes	Usuario no administrador	Usuario administrador
onlyToGateway	Permitir	El túnel se establece automáticamente. El usuario puede cerrar la sesión (sin acceso a la red). El usuario también puede apuntar a otro NetScaler Gateway, en cuyo caso, el acceso se otorga únicamente al NetScaler Gateway que acaba de apuntar.	El túnel se establece automáticamente. El usuario puede desinstalar el cliente Citrix Secure Access o pasar a otro NetScaler Gateway.
onlyToGateway	Negar	El túnel se establece automáticamente. El usuario no puede cerrar la sesión ni apuntar a otro NetScaler Gateway.	El túnel se establece automáticamente. El usuario puede desinstalar el cliente Citrix Secure Access o pasar a otro NetScaler Gateway.

Permitir las URL seleccionadas cuando Always On está inactivo

Los usuarios pueden acceder a algunos sitios web incluso cuando Always On está inactivo y la red está bloqueada. Los administradores pueden usar el registro **AlwaysOnAllowlist** para agregar los sitios web a los que desea habilitar el acceso cuando AlwaysOn esté inactivo.

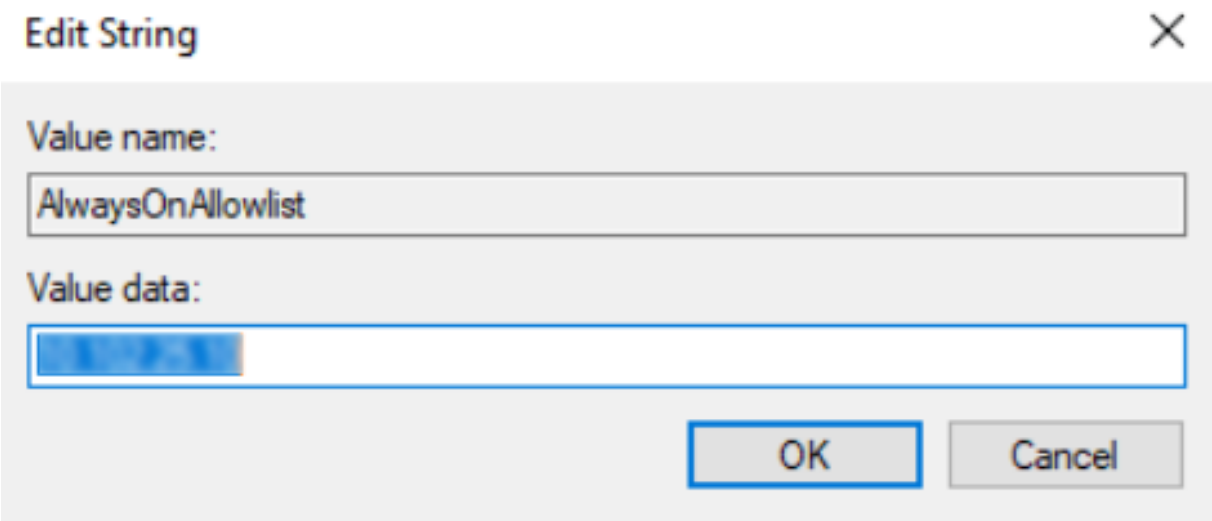
> **Nota:**
>
> - El registro**AlwaysOnAllowlist** se admite desde la versión 13.0 build 47.x y posteriores.
> - La ubicación del registro de**AlwaysOnAllowlist** es Computer\ HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client.
> - Las URLs/FQDN comodín no se admiten en el registro **AlwaysOnAllowlist**.

Para establecer el registro AlwaysOnAllowlist

Configure el registro **AlwaysOnAllowlist** con una lista separada por punto y coma de FQDN, intervalos de direcciones IP o direcciones IP a los que desea permitir el acceso.

Ejemplo: example.citrix.com; 10.103.184.156; 10.102.0.0-10.102.255.100

La siguiente ilustración muestra un registro de ejemplo de **AlwaysOnAllowlist**.



VPN siempre activa antes del inicio de sesión de Windows (formalmente servicio Always On)

January 26, 2024

La función **AlwaysOn VPN antes de iniciar sesión en Windows** (formalmente servicio AlwaysOn) permite al usuario establecer un túnel VPN a nivel de máquina incluso antes de que un usuario inicie sesión en un sistema Windows. El túnel permanece activo hasta que la máquina se apaga. Una vez que el usuario inicia sesión, el túnel de VPN de nivel de máquina se hace cargo de un túnel de VPN de nivel de usuario. Después de que el usuario cierra sesión, el túnel a nivel de usuario se rompe y se establece un túnel a nivel de máquina. **Always On VPN antes de iniciar sesión en Windows** se puede configurar únicamente mediante directivas de autenticación avanzadas. Para obtener más información, consulte Configurar una VPN siempre activa antes del inicio de sesión de Windows.

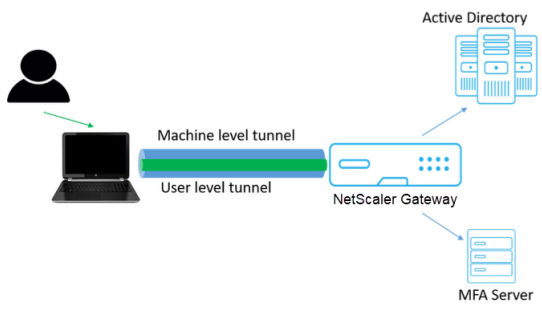
Funciones de Always On VPN antes de iniciar sesión en Windows

- El administrador puede proporcionar una contraseña de un solo uso a los usuarios que trabajan por primera vez de forma remota con la que los usuarios pueden conectarse al controlador de dominio para cambiar su contraseña.
- El administrador puede administrar/aplicar de forma remota las directivas de AD en el dispositivo incluso antes de que el usuario inicie sesión.

- El administrador puede proporcionar un nivel granular de control a los usuarios en función del grupo de usuarios después de que el usuario inicie sesión. Por ejemplo, mediante un túnel de nivel de usuario, puede restringir o proporcionar acceso a un recurso a un grupo de usuarios concreto.
- El túnel de usuario se puede configurar para MFA según los requisitos del usuario.
- Varios usuarios pueden utilizar la misma máquina. El acceso a recursos selectivos se proporciona en función del perfil de usuario. Por ejemplo, varios usuarios pueden utilizar una máquina en un quiosco sin problemas.
- Los usuarios que trabajan de forma remota se conectan al controlador de dominio para cambiar su contraseña.
- La máquina Windows puede verificar la credencial de inicio de sesión del usuario mediante el directorio activo corporativo (AD) y las credenciales de Windows en la máquina no se almacenan en caché. Además, los nuevos usuarios corporativos de AD pueden iniciar sesión sin problemas en el equipo.
- La máquina Windows pasa a formar parte de la intranet corporativa incluso antes de que los usuarios inicien sesión, lo que permite a los administradores de TI acceder al equipo cliente desde la red corporativa con fines de depuración.
- El túnel VPN para una máquina Windows permanece conectado incluso cuando diferentes usuarios inician o citan sesión en el equipo.

Descripción de Always On VPN antes del inicio de sesión de Windows

A continuación se muestra el flujo de eventos de la funcionalidad **Always On VPN antes de iniciar sesión en Windows** .



- El usuario enciende el equipo portátil. El túnel a nivel de máquina se establece hacia NetScaler Gateway mediante el certificado del dispositivo como identidad.
- El usuario inicia sesión en el portátil con las credenciales de AD.
- Después del inicio de sesión, el usuario se enfrenta al desafío de MFA.
- Si la autenticación se realiza correctamente, el túnel de nivel de máquina se sustituye por el túnel de nivel de usuario.

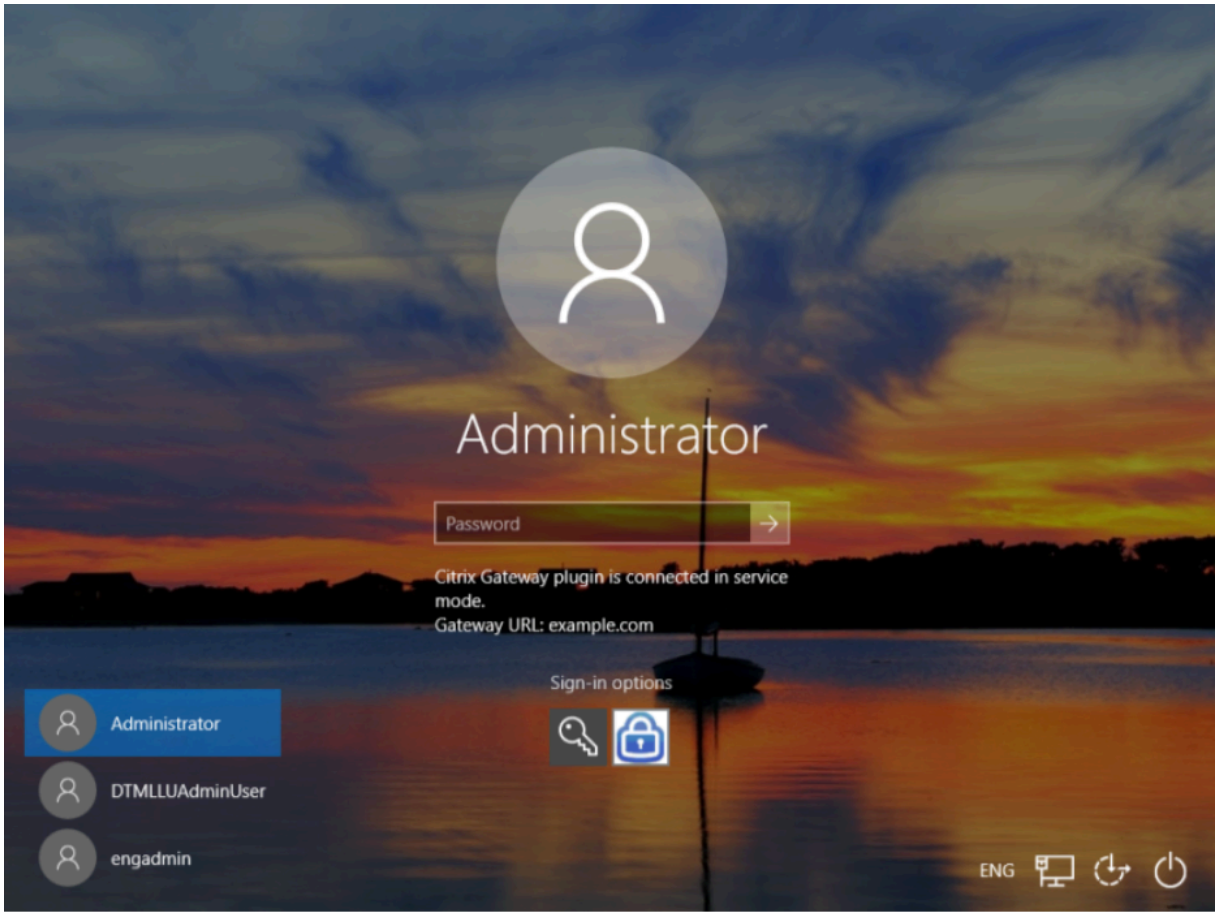
- Una vez que el usuario cierra la sesión, el túnel de nivel de usuario se sustituye por el túnel de nivel de máquina.

Puntos a tener en cuenta:

- El plug-in de VPN y NetScaler Gateway deben ser de la versión 13.0.41.20 y posteriores.
- Si un equipo cliente no tiene conectividad a Internet, **Always On VPN antes de iniciar sesión en Windows** espera a que la conectividad a Internet esté disponible antes de establecer el túnel VPN.
- Si un equipo cliente está conectado a una red de portal cautivo, **Always On VPN antes de iniciar sesión en Windows** espera a que el usuario se autentique en el portal cautivo. Una vez que el usuario inicia sesión y se habilita el acceso a Internet, **Always On VPN antes de iniciar sesión en Windows** establece el túnel VPN.
- La función Always On VPN antes del inicio de sesión de Windows admite portales cautivos para NetScaler.
- Si la opción de credenciales de inicio de sesión almacenadas en caché no está habilitada para Windows, los usuarios no podrán iniciar sesión en los siguientes casos:
  - La máquina no tiene conectividad a Internet
  - El equipo está conectado a una red de portal cautivo
- Los administradores deben comprobar el estado de revocación del certificado del dispositivo antes de presentar la página de inicio de sesión a los usuarios finales.

Pantalla del administrador de credenciales de Windows después de la configuración de Always On VPN antes de iniciar sesión en Windows

Después de configurar la función **Always On VPN before Windows Logon**, la pantalla del **administrador de credenciales de Windows** se modifica de la siguiente manera.



Al hacer clic **en Opciones de inicio** de sesión en la pantalla de inicio de sesión, aparece la siguiente información:

- El icono de NetScaler Gateway indica si la máquina está conectada a NetScaler Gateway o no.
- Según el modo de configuración del usuario, se muestra una de las instrucciones siguientes en la pantalla de inicio de sesión.
  - NetScaler Gateway está conectado en modo de servicio
  - NetScaler Gateway está conectado en modo usuario

Configurar Always On VPN antes del inicio de sesión de Windows

March 27, 2024

En esta sección se capturan los detalles para configurar **Always On VPN antes del inicio de sesión de Windows** mediante una directiva avanzada.

Requisitos previos

- El plug-in de VPN y NetScaler Gateway deben ser de la versión 13.0.41.20 y posteriores.
- Se necesitan NetScaler Advanced Edition y versiones posteriores para que la solución funcione.
- La funcionalidad solo se puede configurar mediante directivas avanzadas.
- El servidor virtual de VPN debe estar en funcionamiento.

Pasos para la configuración

La configuración de **Always On VPN antes de iniciar sesión en Windows** implica los siguientes pasos de alto nivel:

1. Configurar un túnel a nivel de máquina
2. Configurar un túnel a nivel de usuario (opcional)
3. Habilitar autenticación de usuarios

    a) Configure el servidor virtual VPN, instale un certificado de CA y enlace la clave del certificado al servidor virtual.
    b) Creación de un perfil de autenticación
    c) Creación de un servidor virtual de autenticación
    d) Creación de directivas de autenticación
    e) Enlazar las directivas al perfil de autenticación

Túnel a nivel máquina

El túnel a nivel de máquina se establece hacia NetScaler Gateway mediante el certificado del dispositivo como identidad. El certificado del dispositivo debe instalarse en la máquina cliente en el almacén de máquinas. Esto solo se aplica al servicio Always On before Windows Logon.

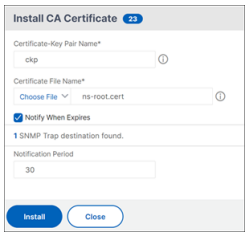
Para obtener más información sobre el certificado de dispositivo, consulte Usar certificados de dispositivo para la autenticación.

> **Importante:**
>
> Si el servidor virtual de VPN del dispositivo NetScaler Gateway está configurado en un puerto no estándar (distinto del 443), el túnel a nivel de máquina no funciona según lo previsto.

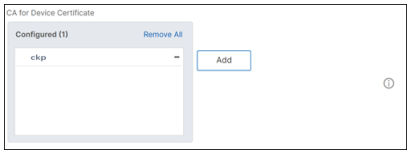
Configurar el túnel a nivel de máquina mediante el certificado de dispositivo

Configuración de autenticación basada en certificados de dispositivo mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **NetScaler Gateway**> Servidores virtuales.
2. **En la página Servidores virtuales de NetScaler Gateway, seleccione un servidor virtual existente y haga clic en Modificar.**
3. En **Certificado**, haga clic en **Certificado de CA**.
4. En la página Vinculación de certificados de **CA**, haga clic en **Agregar** junto al campo **Seleccionar certificado de CA**, actualice la información requerida y haga clic en **Instalar**.



5. En la página **Servidor virtual de VPN**, haga clic en el icono de modificación.
6. En la sección **Configuración básica**, haga clic en **Más**.
7. Haga clic en **Agregar** junto a la sección **CA para certificado de dispositivo** y, a continuación, haga clic en **Aceptar**.



Nota: No active la casilla **Habilitar certificado de dispositivo**.

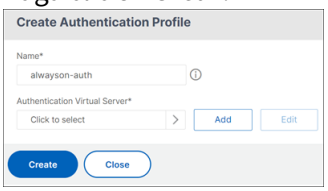
8. Para vincular un certificado de CA al servidor virtual, haga clic en **Certificado de CA** en la sección **Certificado**. Haga clic en **Agregar enlace** en la página **Enlace de certificados de CA de servidor virtual SSL**.

> **Nota:**
>
> - El campo Nombre común del sujeto (CN) del certificado de dispositivo no debe estar vacío. Si un dispositivo intenta iniciar sesión con certificados de dispositivo CN vacíos, su sesión VPN se crea con el nombre de usuario como "anónimo". En IIP, si varias sesiones tienen el mismo nombre de usuario, las sesiones anteriores se desconectan. Por lo tanto, cuando IIP está habilitada, observa el impacto de la funcionalidad debido a un nombre común vacío.
> - Todos los certificados de CA (raíz e intermedia) que pueden firmar potencialmente el certificado de dispositivo emitido a los clientes deben estar enlazados en la sección **CA para certificado de dispositivo** y también en la sección de **enlace de certificados de CA** para el servidor virtual en los pasos 4 y 5. Para obtener más información sobre cómo vincular un certificado de CA con un certificado intermedio o subordinado, con-

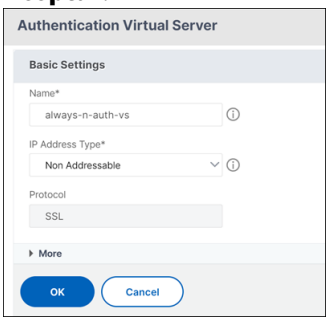
sulte Instalar, vincular y actualizar certificados.

- Si se configuran varios certificados de dispositivos, se intenta el certificado con la fecha de caducidad más larga para la conexión VPN. Si este certificado permite el escaneo de la EPA correctamente, se establece la conexión VPN. Si este certificado falla en el proceso de escaneo, se usa el siguiente certificado. Este proceso continúa hasta que se prueban todos los certificados.

9. En la página **Vinculación de certificados de CA**, seleccione el certificado.
10. Haga clic en **Bind**.
11. Cree un servidor virtual de autenticación.
    a) En la página **Servidores virtuales VPN**, vaya a **Configuración avanzada > Perfil de autenticación** y haga clic en **Agregar**.
    b) En la página **Crear perfil de autenticación**, asigne un nombre al perfil de autenticación y haga clic en **Crear**.



    c) En la página **Servidor virtual de autenticación**, asigne un nombre al servidor virtual de autenticación. Seleccione el tipo de dirección IP como **No direccionable** y haga clic en **Aceptar**.



> **Nota:**
>
> El servidor virtual de autenticación siempre permanece en el estado INACTIVO.

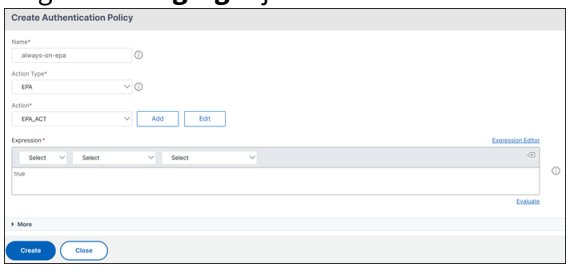
12. Cree una directiva de autenticación.
    a) En la sección **Directivas de autenticación avanzadas** de la página **Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales de autenticación**, seleccione la directiva de autenticación y haga clic en **Agregar enlace**.
    b) En la página Vinculación de **directivas**, haga clic en **Agregar** junto al campo **Seleccionar directiva**.

c) En la página Crear directiva de autenticación ;

i. Asigne un nombre a la directiva de autenticación avanzada.

ii. Seleccione **EPA** en la lista **Tipo de acción**.

iii. Haga clic en **Agregar** junto a **Acción**.

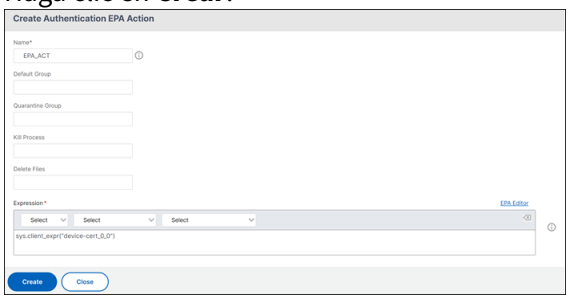


d) En la página Crear acción de autenticación de la EPA;

i. Asigne un nombre a la acción de la EPA.

ii. Introduzca `sys.client_expr("device-cert_0_0")` en el campo **Expresión**.

iii. Haga clic en **Crear**.

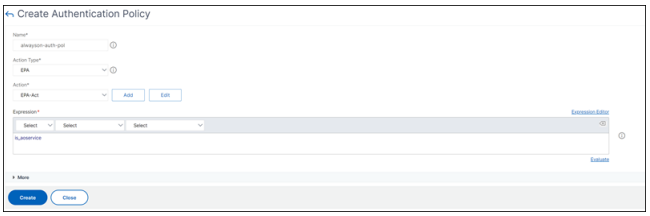


13. En la página **Crear directiva de autenticación** ;

a) Asigne un nombre a la directiva de autenticación.

b) Escriba **is_aoservice** en el campo **Expresión**.

c) Haga clic en **Crear**.



14. En la página Vinculación de directivas, introduzca **100** en **Prioridad** y haga clic en **Vincular**.

Configuración de autenticación basada en certificados de dispositivo mediante la CLI

1. Instale un certificado de CA en un servidor virtual VPN.

```
add ssl certkey ckp -cert t_CA.cer
<!--NeedCopy-->
```


2. Enlazar el certificado de CA al servidor virtual VPN .

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

Ejemplo

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
    -ocspCheck Mandatory
<!--NeedCopy-->
```

3. Agregue un servidor virtual de autenticación.

```
add authentication authnProfile <name>  {
 -authnVsName <string> }

<!--NeedCopy-->
```

Ejemplo

```
add authentication authnProfile always_on -authnVsName
    always_on_auth_server
<!--NeedCopy-->
```

4. Cree una acción de autenticación de la EPA

```
add authentication epaAction <name> -csecexpr <expression>
<!--NeedCopy-->
```

Example

“‘

add authentication epaAction epa-act -csecexpr `sys.client_expr("device-cert_0_0")` -defaultgroup epa_pass

“‘

5. Crear una directiva de autenticación

```
add authentication Policy <name> -rule <expression> -action <
    string>
```

Ejemplo:

```
add authentication Policy always_on_epa_auth -rule is_aoservice -
    action epa_auth
```

> **Importante:**
>
> - La configuración del túnel a nivel de máquina ya está completa. Para configurar el túnel de nivel de usuario después del inicio de sesión de Windows, consulte la sección **Túnel de**

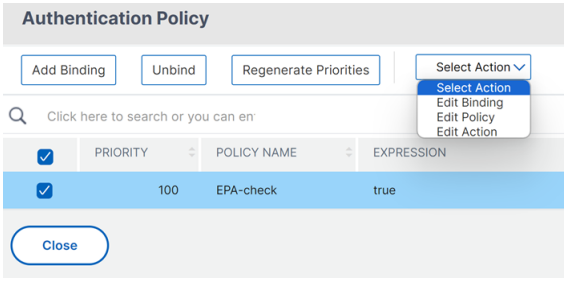
> **nivel de usuario**.
>
> - En el equipo cliente, el certificado del dispositivo está en formato.pfx. El certificado.pfx se instala en la máquina Windows, ya que Windows entiende el formato.pfx. Este archivo contiene los archivos de certificado y clave. Este certificado debe ser del mismo dominio que está enlazado al servidor virtual. Los certificados y claves.pfx y de servidor se pueden generar mediante el asistente para certificados de cliente. Estos certificados se pueden usar con la entidad de certificación para generar el.pfx respectivo con el certificado del servidor y el dominio. El certificado.pfx se instala en la cuenta de equipo en la carpeta personal. El comando `show aaa session`muestra el túnel del dispositivo en el dispositivo NetScaler.

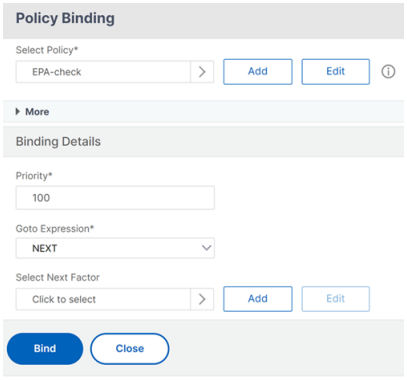
Túnel a nivel usuario

Reemplazar un túnel de nivel de máquina por un túnel de nivel de usuario mediante la interfaz gráfica de usuario

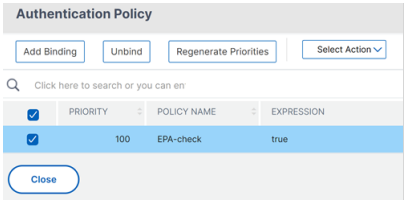
Nota: La expresión `is_aoservice.not`se aplica a partir de la versión 13.0.41.20 y posteriores de NetScaler Gateway.

1. Configure una directiva para la autenticación de usuarios.
   a) Vaya a **NetScaler Gateway > Servidores** virtuales y seleccione un servidor virtual.
   b) En **Configuración avanzada**, haga clic en **Perfil de autenticación**.
   c) Configure el perfil de autenticación.
   d) En la página **Configuración > Seguridad > Tráfico de aplicaciones AAA > Servidores virtuales de autenticación**, seleccione la directiva de autenticación.
   e) En **Seleccionar acción**, haga clic en **Modificar enlace** y cambie **Expresión GoTo** a **SIGUIENTE** en lugar de **END** para el límite de la directiva.





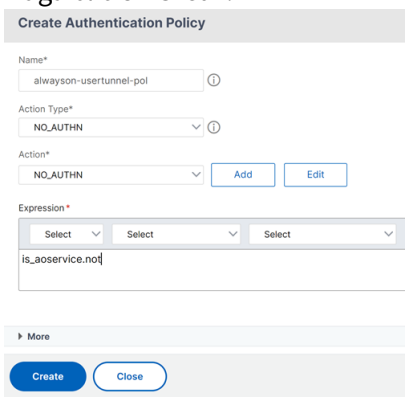
f) Haga clic en **Enlazar** y, a continuación, en la página **Directiva de autenticación**, seleccione la directiva de autenticación y haga clic en **Agregar enlace**.



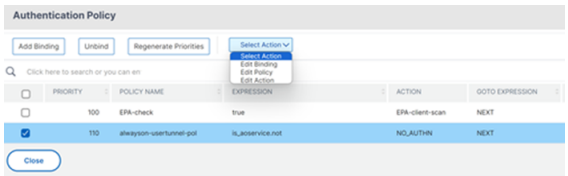
g) En la página Vinculación de directivas, haga clic en **Agregar** junto a **Seleccionar directiva**.

En la página Crear directiva de autenticación ;

i. Introduzca un nombre para la directiva “sin autenticación”que se va a crear.
ii. Seleccione el tipo de acción como **no_Authn**.
iii. Escriba **is_aoservice.not** en el campo **Expresión**.
iv. Haga clic en **Crear**.



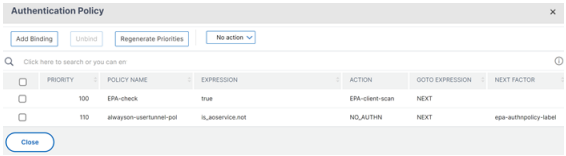
2. En **Seleccionar acción**, haga clic en **Modificar enlace**.



3. En la página Vinculación de directivas, introduzca **110** en **Prioridad**. Haga clic en **Agregar** junto a **Seleccionar siguiente factor**.

   a) En la página Etiqueta de directiva de autenticación, introduzca un nombre descriptivo para la etiqueta de directiva, seleccione el esquema de inicio de sesión y haga clic en **Continuar**.
   b) En **Seleccionar directiva**, haga clic en **Agregar** y cree una directiva de autenticación LDAP.
   c) Haga clic en **Crear y,** a continuación, en **Enlazar.**
   d) Haga clic en **Listo y,** a continuación, en **Enlazar**.

   En la página Directiva de autenticación, la columna **Factor siguiente** muestra la directiva de siguiente factor configurada.



4. Puede configurar la directiva LDAP como el siguiente factor de la directiva de autenticación.

   a) En la página Crear directiva de autenticación, introduzca un nombre para la directiva LDAP.
   b) Seleccione **Tipo de acción** como **LDAP**.
   c) Introduzca **Acción como acción** LDAP configurada.

> **Nota:**
>
> - Para crear un archivo XML de esquema de inicio de sesión, consulte Archivo XML de esquemade inicio
> - Para crear etiquetas de directiva, consulte Autenticar la etiqueta de directiva.
> - Para crear una directiva de autenticación LDAP, consulte Para configurar la autenticación LDAP mediante la utilidad de configuración.

Reemplazar un túnel de nivel de máquina por un túnel de nivel de usuario mediante la CLI

1. Enlazar una directiva al servidor virtual de autenticación

```
bind authentication vserver <name> -policy <name> -priority  <
    positive_integer> -gotoPriorityExpression <expression>
```

   Ejemplo

```
bind authentication vserver alwayson-auth-vserver -policy alwayson
    -auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. Agregue una directiva de autenticación con la acción como `NO_AUTH`y la expresión `is_aoservice.not`, y enlácela a la directiva.


```
add authentication Policy <name> -rule <expression> -action <
    string>

bind authentication vserver <name> -policy <name> -priority <
    positive_integer> -gotoPriorityExpression <expression>
```

Ejemplo

```
add authentication Policy alwayson-usertunnel-pol -rule
    is_aoservice.not -action NO_AUTHN

bind authentication vserver alwayson-auth-vserver -policy alwayson
    -usertunnel-pol -priority 110
```

3. Agregue un factor siguiente y vincule la etiqueta de la directiva al siguiente factor.

```
add authentication policylabel <labelName> -loginSchema <string>

bind authentication  policylabel <string>  -policyName <string>  -
    priority <positive_integer> -gotoPriorityExpression <expression
    > -nextFactor <string>
```

Ejemplo

```
add authentication policylabel user-tunnel-auth-label -loginSchema
     singleauth_alwayson

bind authentication policylabel user -policyName alwayson-
    usertunnel-pol -priority 100
```

4. Configure una directiva LDAP y enlácela a la etiqueta de directiva de túnel de usuario.

```
add authentication policy <name>  -rule <expression>  -action <
    string>

bind authentication vserver <vserver_name> -policy <string>  -
    priorit < positive integer>  gotoPriorityExpression <string>
```

Ejemplo

```
add authentication Policy LDAP_new -rule true -action LDAP_new

bind authentication policylabel user-tunnel-auth-label -policyName
     LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

Configuración del lado del cliente

Los Registros `AlwaysOn`, `locationDetection`, `and suffixList registries`son opcionales y solo se requieren si se necesita la funcionalidad de detección de ubicación.

Para acceder a las entradas de clave de registro, vaya a la siguiente ruta: **Computer>HKEY_LOCAL_MACHINE>SOF**
Access Client

Clave del Registro	Tipo de Registro	Valores y descripción
AlwaysOnService	REG_DWORD	1 => Establecer túnel a nivel máquina pero no túnel a nivel de usuario; 2 => Establecer túnel a nivel máquina y túnel a nivel de usuario
AlwaysOnURL	REG SZ	URL del servidor virtual de NetScaler Gateway al que el usuario quiere conectarse. **Ejemplo:** `https://xyz.companyDomain.com` **Importante:** Solo una URL es responsable del túnel a nivel de máquina y del túnel a nivel de usuario. El registro AlwaysOnURL ayuda tanto al servicio como al componente de nivel de usuario a funcionar y a conectar un túnel independiente, es decir, túnel a nivel de máquina y túnel a nivel de usuario según el diseño
AlwaysOn	REG_DWORD	1 => Permitir el acceso a la red en caso de fallo de VPN; 2=> Bloquear el acceso a la red si falla
AlwaysOnAllowlist	REG_SZ	Lista de direcciones IP o FQDN separados por punto y coma que deben incluirse en la lista de permitidos mientras la máquina se ejecuta en modo estricto. **Ejemplo:** `8.8.8.8;linkedin.com`

Clave del Registro	Tipo de Registro	Valores y descripción
UserCertCAList	REG_SZ	Lista de nombres de CA raíz separados por comas o puntos y coma, es decir, el nombre del emisor del certificado. Se utiliza en el contexto de un servicio Always On, en el que un cliente puede especificar la lista de CA para elegir el certificado de cliente. **Ejemplo**: `cgwsanity.net;xyz.gov.in`
locationDetection	REG_DWORD	1 => Para habilitar la detección de ubicación; 0 => Para inhabilitar la detección de ubicación
suffixList	REG SZ	Lista de dominios separada por punto y coma y se encarga de comprobar si la máquina está en la intranet o no en un momento dado cuando la detección de ubicación está habilitada. **Example:** `citrite.net,cgwsanity.net`

Para obtener más información sobre estas entradas del registro, consulte Siempre activado.

> **Nota:**
>
> Cuando se configura el servicio Always On, el perfil Always On configurado en el servidor virtual de NetScaler Gateway o en NetScaler se ignora en el lado del cliente. Por lo tanto, asegúrese de habilitar también los `locationDetection`registros `AlwaysOn`y VPN al configurar el servicio Always On.
> ‘‘‘

Usar la directiva avanzada para crear directivas VPN

January 26, 2024

Classic Policy Engine (PE) y Advance Policy Infrastructure (PI) son dos marcos de configuración y evaluación de directivas diferentes que NetScaler admite actualmente.

La infraestructura de directivas avanzadas consiste en un potente lenguaje de expresión. El lenguaje de expresión se puede utilizar para definir reglas en la directiva, definir varias partes de Action y otras entidades admitidas. El lenguaje de expresión puede analizar cualquier parte de la solicitud o respuesta y también le permite examinar en profundidad los encabezados y la carga útil. El mismo lenguaje de expresiones se expande y funciona en todos los módulos lógicos compatibles con NetScaler.

> **Nota:**
> Le recomendamos que utilice directivas avanzadas para crear directivas.

¿Por qué migrar de la directiva clásica a la directiva anticipada?

Advanced Policy tiene un conjunto de expresiones enriquecido y ofrece una flexibilidad mucho mayor que la directiva clásica. A medida que NetScaler escala y atiende a una amplia variedad de clientes, es imprescindible admitir expresiones que superen ampliamente las directivas avanzadas. Para obtener más información, consulte Directivas y expresiones.

A continuación se presentan las capacidades agregadas para la Directiva Anticipada.

- Posibilidad de acceder al cuerpo de los mensajes.
- Es compatible con muchos otros protocolos.
- Accede a muchas otras funciones del sistema.
- Tiene más funciones básicas, operadores y tipos de datos.
- Permite analizar archivos HTML, JSON y XML.
- Facilita la rápida coincidencia paralela de múltiples cadenas (`patsets`y así sucesivamente).

Ahora se pueden configurar las siguientes directivas de VPN mediante Advance Policy.

- Directiva de sesión
- Directiva de autorización
- Directiva de tráfico
- Directiva de túnel
- Directiva de auditoría

Además, el análisis de punto final (EPA) se puede configurar como una función nFactor para autenticación. La EPA se utiliza como control de acceso para los dispositivos de punto final que intentan

conectarse al dispositivo Gateway. Antes de que se muestre la página de inicio de sesión de la puerta de enlace en un dispositivo de punto final, se comprueban los requisitos mínimos de hardware y software del dispositivo, en función de los criterios de elegibilidad configurados por el administrador de la puerta de enlace. El acceso a la puerta de enlace se concede en función del resultado de las comprobaciones realizadas. Anteriormente, EPA se configuraba como parte de la directiva de sesión. Ahora se puede vincular a nFactor proporcionando más flexibilidad en cuanto a cuándo se puede realizar. Para obtener más información sobre la EPA, consulte el tema Cómo funcionan las directivas de dispositivos de punto final. Para obtener más información sobre nFactor, consulte el tema Autenticación nFactor.

Casos de uso:

EPA previo a la autenticación mediante EPA avanzado

El escaneo de EPA previo a la autenticación se realiza antes de que el usuario proporcione las credenciales de inicio de sesión. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con el escaneo de EPA previo a la autenticación como uno de los factores de autenticación, consulte el tema CTX224268.

EPA posterior a la autenticación mediante EPA avanzada

La exploración EPA posterior a la autenticación se realiza después de verificar las credenciales de usuario. En la infraestructura de directivas clásica, la EPA posterior a la autenticación se configuró como parte de la directiva de sesión o de la acción de sesión. En la infraestructura de directivas avanzada, la exploración EPA se configurará como factor EPA en la autenticación nFactor. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con la exploración EPA posterior a la autenticación como uno de los factores de autenticación, consulte el tema CTX224303.

EPA de autenticación previa y versiones posteriores a la autenticación mediante directivas avanzadas

EPA se puede realizar antes de la autenticación y versiones posteriores a la autenticación. Para obtener información sobre cómo configurar NetScaler Gateway para la autenticación nFactor con exploraciones EPA previas y posteriores a la autenticación, consulte el tema CTX231362.

Escaneo periódico de la EPA como factor en la autenticación nFactor

En la infraestructura de directivas clásica, el análisis periódico de EPA se configuró como parte de la acción de directiva de sesión. En la infraestructura de directivas avanzada, se puede configurar como

parte del factor EPA en la autenticación nFactor.

Para obtener más información sobre cómo configurar la exploración EPA periódica como factor en la autenticación nFactor, haga clic en el temaCTX231361.

Solución de problemas:

Los siguientes puntos deben tenerse en cuenta para la solución de problemas.

- Las directivas clásicas y avanzadas del mismo tipo (por ejemplo, directiva de sesión) no pueden vincularse a la misma entidad o punto de enlace.
- La prioridad es obligatoria para todas las directivas de PI.
- La directiva anticipada para la VPN se puede vincular a todos los puntos de enlace.
- La directiva anticipada con la misma prioridad se puede vincular a un único punto de enlace.
- Si no se selecciona ninguna de las directivas de autorización configuradas, se aplica la acción de autorización global configurada en el parámetro VPN.
- En la directiva de autorización, la acción de autorización no se invierte si se produce un error en la regla de autorización.

Expresiones equivalentes de directivas avanzadas de uso común para Classic Policy:

Expresiones clásicas de directivas	Expresiones de directiva anticipada
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER “foo”	HEADER(“foo”)
CONTAINS ”bar”	.CONTAINS («bar») [Tenga en cuenta el uso de «..»]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS

Expresiones clásicas de directivas	Expresiones de directiva anticipada
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

Configurar el servidor virtual de VPN DTLS mediante el servidor virtual de VPN SSL

March 27, 2024

Puede configurar un servidor virtual VPN DTLS para NetScaler Gateway con la misma dirección IP y número de puerto que un servidor virtual VPN SSL configurado. La configuración de servidores virtuales DTLS VPN le permite vincular los cifrados y certificados DTLS avanzados al tráfico DTLS para mejorar la seguridad.

> **Importante:**
>
> - De forma predeterminada, la funcionalidad DTLS está activada para el servidor virtual SSL VPN existente. Inhabilite la funcionalidad del servidor antes de crear el servidor virtual de VPN DTLS.
> - El servidor virtual de puerta de enlace SNI para DTLS se admite en NetScaler Gateway versión 13.0 compilación 64.x y posteriores.
> - A partir de la versión 13.0 compilación 79.x de NetScaler, el parámetro `helloverifyrequest` está habilitado de forma predeterminada. Habilitar el parámetro `helloverifyrequest` en el perfil DTLS ayuda a mitigar el riesgo de que un atacante o bots abruman el rendimiento de la red, lo que podría provocar un agotamiento del ancho de banda saliente. Es decir, ayuda a mitigar el ataque de amplificación DDoS DTLS. Para obtener más información sobre el parámetro `helloverifyrequest`, consulte Perfil DTLS.
> - Al controlar el tráfico UDP, el consumo de memoria del dispositivo NetScaler aumenta si los servidores back-end impulsan mucho tráfico. Como resultado, el dispositivo NetScaler no puede enviar este tráfico al cliente debido a la conexión TCP MUX en el lado del cliente. En tales casos, Citrix recomienda utilizar el protocolo DTLS.

Puntos que tener en cuenta

- El servidor virtual de VPN DTLS en un dispositivo con NetScaler Gateway se puede configurar a partir de la versión 13.0, compilación 58.x.

- Antes de configurar un servidor virtual de VPN DTLS en un dispositivo con NetScaler Gateway, debe haber configurado un servidor virtual de VPN SSL en el dispositivo.
- El servidor virtual de VPN de DTLS utiliza la dirección IP y el número de puerto del servidor virtual de VPN SSL configurado.
- Si se produce un error en el protocolo de enlace DTLS, la conexión vuelve a ser TLS.
- Para usar solo DTLS, puede inhabilitar TLS vinculando solo los cifrados DTLS al tráfico DTLS.
- La multiplexación DTLS no se admite cuando el tráfico TCP se canaliza a través de una VPN.

Configurar un servidor virtual VPN con DTLS mediante la GUI

1. En la pestaña Configuración, vaya a **NetScaler Gateway > Servidores virtuales**.
2. En la página **Servidores virtuales de NetScaler Gateway**, seleccione el servidor virtual SSL VPN existente y haga clic en **Modificar**.
3. En la página **Servidor virtual VPN**, haga clic en el icono de edición, desactive la casilla de verificación **DTLS** y haga clic en **Aceptar**.
4. Vuelva a **NetScaler Gateway > Servidores virtuales** y haga clic en **Agregar**.
5. En **Configuración básica**, introduzca los valores de los campos siguientes y haga clic en **Aceptar**.
    - Nombre: nombre para el servidor virtual de VPN de DTLS
    - Protocolo: Seleccione DTLS
    - Dirección IP: Introduzca la dirección IP del servidor virtual VPN SSL
    - Puerto: Introduzca el número de puerto del servidor virtual VPN SSL
6. En la página **Servidores virtuales de NetScaler Gateway**, seleccione el servidor virtual que agregó anteriormente y haga clic en **Modificar**.
7. En **Certificados**, haga clic en el icono de flecha para seleccionar la clave de certificado requerida.
8. En **Vinculación de certificados de servidor > Seleccionar certificado de servidor**, seleccione una clave de certificado SSL existente o cree una.
9. Haga clic en **Enlazar** en la página **Enlace de certificado de servidor**.

> **Nota:**
>
> - Para usar DTLS 1.2, haga clic en el icono de modificación en Parámetros SSL y seleccione la casilla de verificación **DTLS 1.2**.
> - La indicación del nombre del servidor (SNI) es compatible con el servidor virtual de VPN de

> tipo DTLS.

Configurar un servidor virtual VPN DTLS mediante la CLI

En la línea de comandos, escriba el siguiente conjunto de comandos:

```
set vpn vserver <ssl vpnvserver name> -dtls off
add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn vserver port>
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key>
<!--NeedCopy-->
```

DTLS 1.0 funciona como de costumbre, para usar DTLS 1.2, escriba el siguiente comando:

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
<!--NeedCopy-->
```

Ejemplo

```
set vpn vserver vpnvserver  -dtls off
add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443
bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey
set ssl vserver vpnvserver_dtls -dtls12 ENABLED
<!--NeedCopy-->
```

Para habilitar SNI para el servidor virtual de VPN de tipo DTLS, escriba el siguiente comando:

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key> <-SNICert>
<!--NeedCopy-->
```

Ejemplo

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED
bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/*.insight.net.cer_CERT_" -snICert

<!--NeedCopy-->
```

Parámetros de servidor virtual DTLS VPN compatibles

Solo se admiten los siguientes parámetros para el servidor virtual VPN de tipo DTLS.

- Ipaddress
- Puerto
- State

- Doble salto
- downstateflush
- Comment
- Appflowlog
- Icmpvsrresponse

Parámetros de servidor virtual DTLS VPN no compatibles

Los siguientes parámetros no son compatibles con el servidor virtual VPN de tipo DTLS.

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- l2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

Configurar un servidor virtual DTLS mediante el asistente de XenApp y XenDesktop

1. Haga clic en **XenApp y XenDesktop** en **Integrar en productos Citrix**.
2. En el asistente de configuración de XenApp y XenDesktop, seleccione **StoreFront** y haga clic en **Continuar**.

3. En la página **Configuración de NetScaler Gateway**, active la casilla de verificación **Configurar un agente de escucha DTLS para este servidor virtual de VPN** y haga clic en **Continuar**.

   La escucha DTLS ya está configurada.

4. En Certificado de servidor, haga clic en **Elegir archivo** para seleccionar el certificado de servidor y haga clic en **Continuar**.
5. Especifique el archivo de certificado y el nombre del archivo clave y haga clic en **Continuar**.
6. En la sección **StoreFront**, proporcione los valores de los parámetros necesarios de la siguiente manera y haga clic en **Continuar**.
7. En la sección **Autenticación**, proporcione los valores de los parámetros requeridos de la siguiente manera y haga clic en **Probar conexión**.

   Asegúrese de que el servidor es accesible, proporcione el valor de tiempo de espera y el atributo Nombre de inicio de sesión del servidor y haga clic en **Continuar**.

8. Haga clic en **Listo** para completar la configuración.

Limitaciones

- DTLS 1.2 solo es compatible con clientes Windows.
- El servidor virtual de VPN con DTLS no admite direcciones IPv6.
- La directiva SSL y el perfil SSL no son compatibles con un servidor virtual de VPN de DTLS. Además, no se admite el enlace de la directiva de servidor virtual de VPN.
- El servidor virtual de VPN DTLS de NetScaler Gateway no admite las siguientes funciones. Sin embargo, el servidor virtual de VPN SSL de NetScaler Gateway admite estas funciones:
  - Gateway unificado con servidor virtual de cambio de contenido
  - UDP MUX
  - Vídeo UDP
  - Audio UDP
  - PCOIP
- No se admite el comando `stat vpn vserver` relacionado con las estadísticas del servidor virtual de VPN DTLS.
- Las claves HSM no se admiten en el servidor virtual DTLS.
- No se admite la configuración de clústeres.

Integración con los productos de NetScaler

January 26, 2024

Si es un administrador del sistema responsable de instalar y configurar NetScaler Gateway, puede configurar el dispositivo para que admita Citrix Endpoint Management, StoreFront y la interfaz web.

Los usuarios pueden conectarse directamente a Endpoint Management desde la red interna o desde una ubicación remota. Cuando los usuarios se conectan, pueden acceder a sus aplicaciones web, SaaS y móviles. También pueden admitir documentos ubicados en ShareFile desde cualquier dispositivo.

Para permitir las conexiones de usuarios a una comunidad de servidores a través de NetScaler Gateway, configure los valores en StoreFront o en la Interfaz Web y en NetScaler Gateway. Cuando los usuarios se conectan, tienen acceso a aplicaciones publicadas y escritorios virtuales.

Los pasos de configuración para integrar NetScaler Gateway con Endpoint Management, StoreFront y la interfaz web suponen lo siguiente:

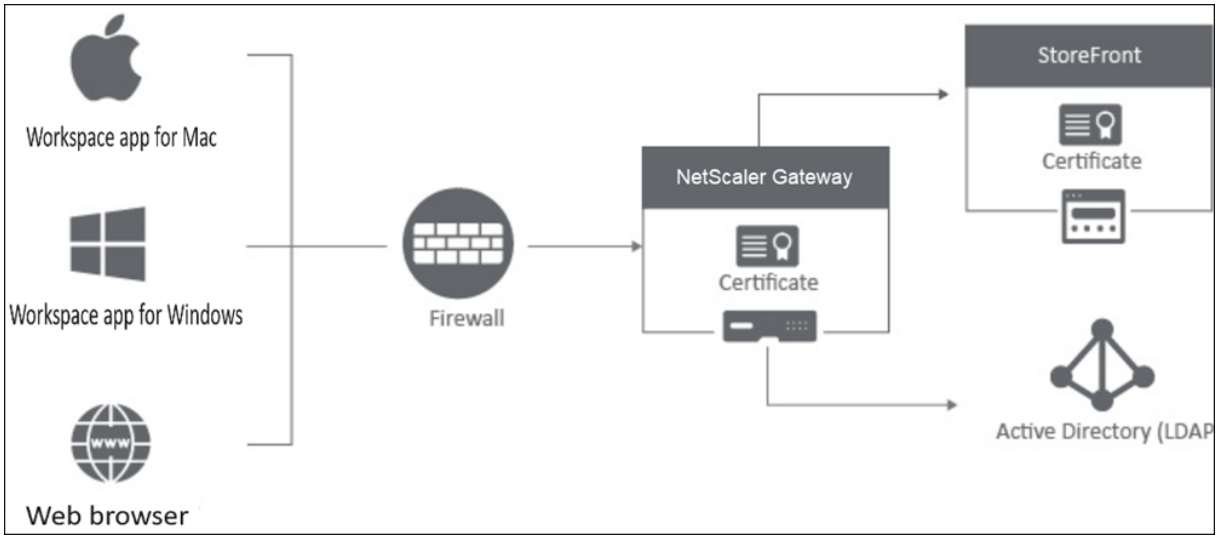
- NetScaler Gateway reside en la DMZ y está conectado a una red existente.
- NetScaler Gateway se implementa como dispositivo independiente y los usuarios remotos se conectan directamente a NetScaler Gateway.
- StoreFront, Endpoint Management, Citrix Virtual Apps, Citrix Virtual Desktops y la interfaz web residen en la red segura.
- ShareFile se configura en Endpoint Management. Para obtener más información sobre ShareFile, consulte el tema ShareFile y el tema Configuración de ShareFile para el acceso de usuario.

La forma de implementar StoreFront y Endpoint Management depende de las aplicaciones que proporcione a los dispositivos móviles. Si los usuarios tienen acceso a aplicaciones MDX empaquetadas con MDX Toolkit, Endpoint Management reside delante de StoreFront en la red segura. Si no proporciona acceso a las aplicaciones MDX, StoreFront reside delante de Endpoint Management en la red segura.

Integrar NetScaler Gateway en StoreFront

March 27, 2024

En este artículo se describe cómo crear un servidor virtual NetScaler Gateway para acceder de forma remota a StoreFront, para los usuarios que utilizan la aplicación Citrix Workspace o un explorador web.



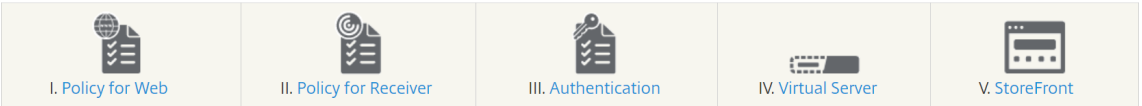
Los usuarios se conectan a NetScaler Gateway a través de un explorador web o la aplicación Citrix Workspace. NetScaler Gateway autentica a los usuarios en función de las directivas configuradas. Si la autenticación se realiza correctamente, NetScaler Gateway permite a los usuarios iniciar sesión de forma única en el almacén y envía el almacén de StoreFront al usuario.

> **Importante:**
>
> Se recomienda no utilizar el asistente Citrix Virtual Apps and Desktops para integrar NetScaler Gateway con StoreFront, ya que crea una configuración no válida mediante las directivas de autenticación clásicas (en desuso).

Configurar NetScaler Gateway para utilizarlo con StoreFront

Para integrar NetScaler Gateway con StoreFront, siga estos pasos:

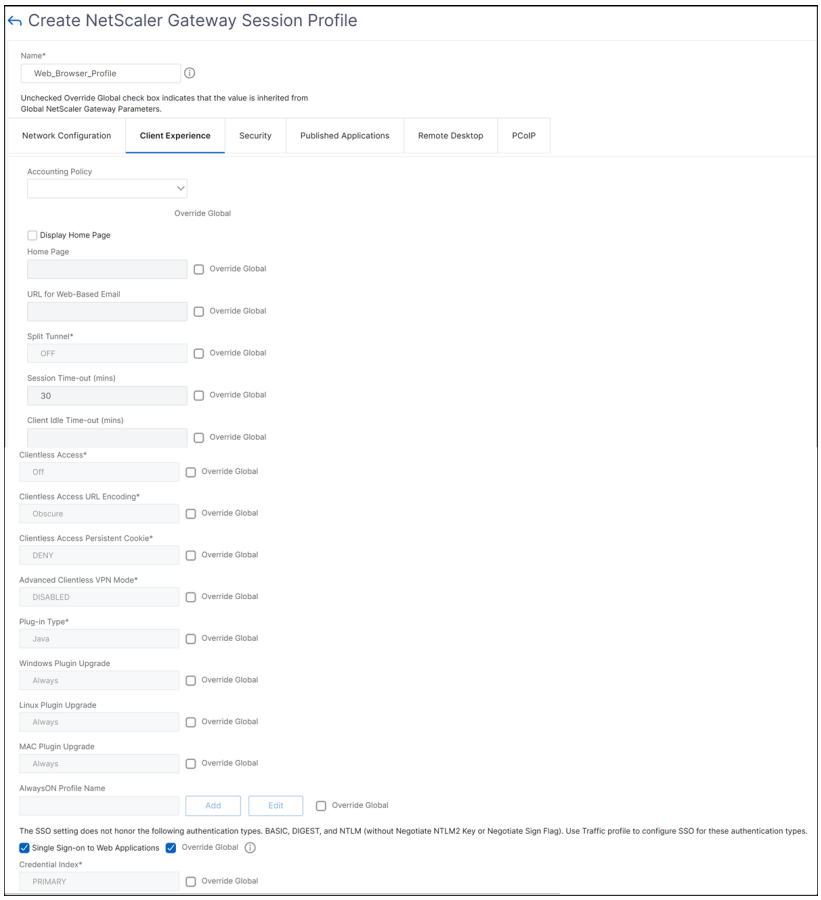
1. Crear una directiva de sesión para el acceso basado en explorador web
2. Crear una directiva de sesión para el acceso basado en la aplicación Citrix Workspace
3. Creación de un perfil de autenticación
4. Crear un servidor virtual de NetScaler Gateway
5. Agregue la instancia de NetScaler Gateway en StoreFront



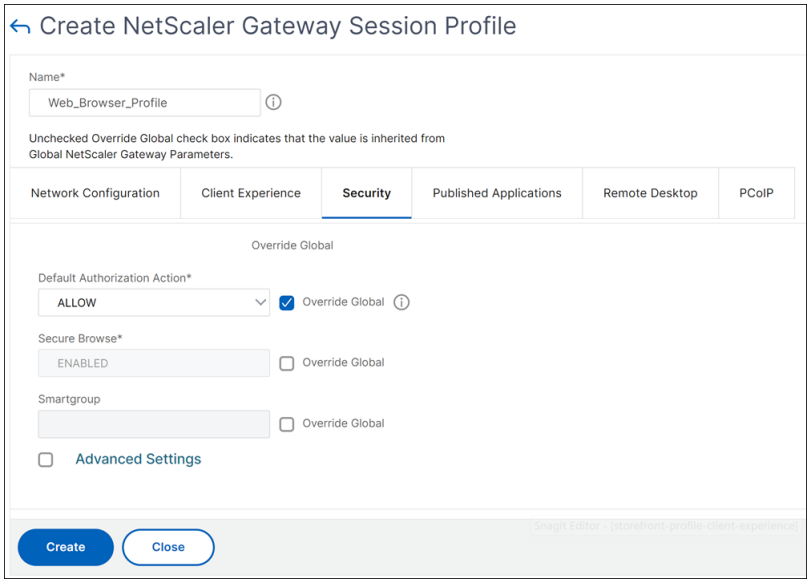
1. Crear una directiva de sesión para el acceso basado en explorador web

1. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.

2. En la ficha **Perfiles de sesión**, haga clic en **Agregar**.
3. Asigne un nombre al perfil de sesión.
4. En la ficha **Experiencia del cliente**, active la siguiente configuración:
   - **Tipo de complemento : el tipo**de complemento se establece en **Java** de forma predeterminada. Aunque esta configuración es opcional, se recomienda si los usuarios desean inhabilitar la VPN completa.
   - **Inicio de sesión único en la aplicación**web: al seleccionar esta opción, cuando un usuario inicia sesión en NetScaler Gateway, reenvía las credenciales al sitio web de StoreFront. Esta configuración evita que los usuarios tengan que introducir sus credenciales dos veces. Sin embargo, también debe habilitar el método de autenticación PassThrough desde NetScaler Gateway en StoreFront. Inhabilite esta opción si necesita que los usuarios inicien sesión en NetScaler Gateway y en el almacén de StoreFront con credenciales diferentes.

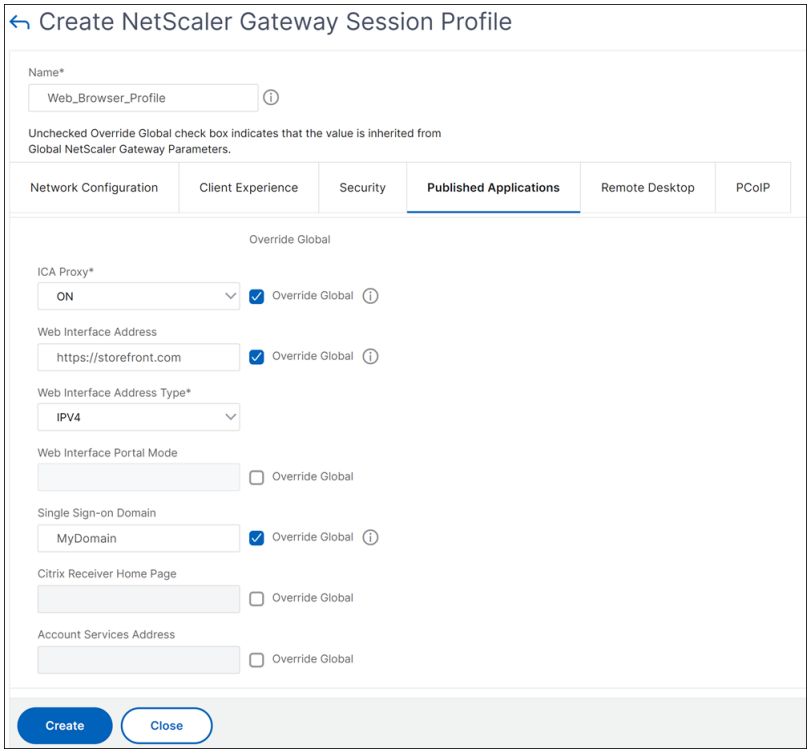


5. En la ficha **Seguridad**, habilite la **Acción de autorización predeterminada** y configúrela en **PERMITIR**.



6. En la ficha **Aplicaciones publicadas**, habilite estos parámetros:

   - **Proxy ICA**: establecido en ON.
   - **Dirección de interfaz web:** FQDN del servidor de StoreFront seguido de la ruta de acceso al sitio web del almacén.
   - **Dominio de inicio de sesión único**: Si solo usa un dominio, si quiere, introduzca el nombre NetBIOS del dominio.

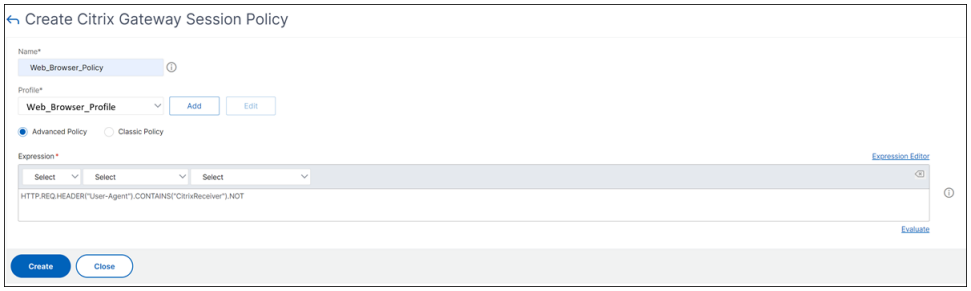


7. Haga clic en **Crear**.

8. En la ficha **Directivas de sesión**, haga clic en **Agregar**. La directiva de sesión es necesaria para que NetScaler diferencie entre las conexiones basadas en el explorador web y las basadas en la aplicación Citrix Workspace. Esta directiva se aplica a las conexiones basadas en exploradores web.
9. En **Nombre**, asigne un nombre a la directiva de sesión.
10. En **Perfil**, seleccione el perfil de sesión que creó.
11. Haga clic en la opción **Directiva avanzada** e introduzca la siguiente sintaxis en **Expresión** :

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
    ```

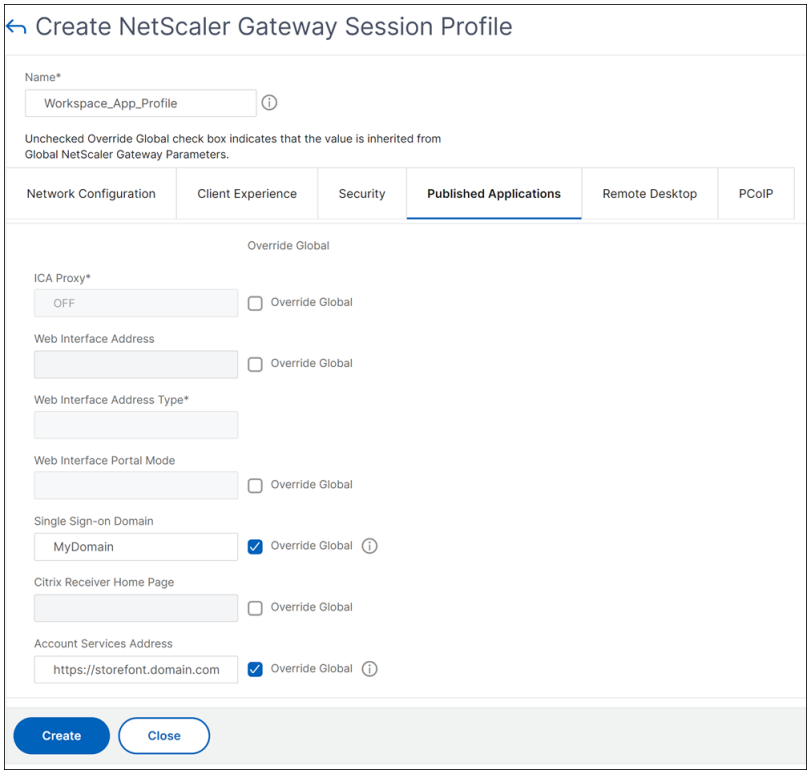
12. Haga clic en **Crear**.



Para obtener más información sobre las directivas de sesión de NetScaler Gateway, consulte Directivas de sesión.

2. Crear una directiva de sesión para el acceso basado en la aplicación Citrix Workspace

Repita los pasos anteriores para crear una directiva de sesión y un perfil de sesión para el acceso basado en la aplicación Citrix Workspace. Sin embargo, en la ficha **Aplicaciones publicadas**, en lugar de configurar la dirección de la interfaz web, debe configurar la **dirección del servicio de cuentas**. Este paso requiere que proporcione el FQDN del servidor StoreFront. La aplicación Citrix Workspace usa esta dirección para detectar los almacenes que están disponibles en el servidor.



3. Creación de un perfil de autenticación

Cree un perfil de autenticación en NetScaler según el tipo de método de autenticación que necesite configurar.

Aunque este paso es opcional, se recomienda utilizar NetScaler Gateway para autenticar la identidad de los usuarios antes de conceder el acceso a StoreFront.

Consulte Autenticación y autorización para obtener más información.

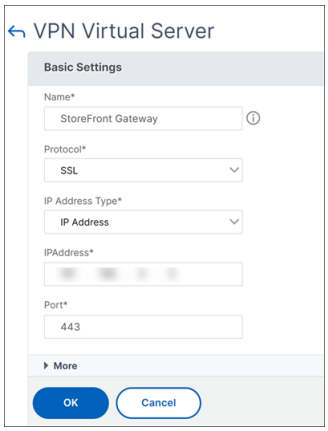
4. Crear un servidor virtual de NetScaler Gateway

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. Haga clic **en**Agregar para agregar un servidor virtual de NetScaler Gateway.
3. Asigne un nombre y una dirección al servidor virtual.

   > **Nota:**
   >
   > Si decide no usar NetScaler Gateway para autenticar a los usuarios, haga clic en **Más** y desactive la casilla de verificación **Habilitar autenticación**.

4. En **Certificado**, haga clic en **Certificado de servidor**.

5. Cargue un certificado de servidor y haga clic en **Vincular**.
6. Agregue las directivas de sesión:
    a) En **Directivas**, haga clic en **+**.
    b) En la lista desplegable **Elegir directiva**, seleccione **Sesión**. En la lista desplegable **Tipo**, seleccione **Solicitud** y, a continuación, haga clic en **Continuar**.
    c) En **Vinculación de directivas**, haga clic en **Seleccionar directiva** y seleccione la directiva de sesión basada en el explorador web y la directiva de sesión basada en la aplicación Citrix Workspace que creó anteriormente y haga clic en **Vincular** para vincular las directivas de sesión al servidor virtual.
7. En **Aplicaciones publicadas**, haga clic en **STA Server**. Especifique al menos una URL de Security Ticket Authority (STA). Si usa Citrix Virtual Apps and Desktops, introduzca las URL de los Desktop Delivery Controllers. Si utiliza Citrix DaaS, introduzca las URL de los Citrix Cloud Connectors.
8. En **Perfil de autenticación**, seleccione el perfil de autenticación que creó. Este paso es obligatorio porque ya no se admiten las directivas clásicas.
9. Haga clic en **Listo**.



5. Agregar una instancia de NetScaler Gateway en StoreFront

Para obtener instrucciones sobre cómo agregar una instancia de NetScaler Gateway en StoreFront, consulte Configurar NetScaler Gateways.

Referencias

Para obtener más información sobre la integración de StoreFront y NetScaler Gateway, consulte los siguientes temas:

- Agregar NetScaler Gateway
- Diseño de la integración de StoreFront y NetScaler Gateway

Integrar NetScaler Gateway en Citrix Virtual Apps and Desktops

January 26, 2024

Los servidores de StoreFront se implementan y se configuran para administrar el acceso a los datos y los recursos publicados. Para el acceso remoto, se recomienda agregar NetScaler Gateway y colocarlo delante de StoreFront.

> **Nota**
>
> Para obtener pasos de configuración detallados sobre cómo integrar Citrix Virtual Apps and Desktops con NetScaler Gateway, consulte ladocumentación de StoreFront.

En el siguiente diagrama se muestra un ejemplo de implementación de Citrix simplificada de Citrix que incluye NetScaler Gateway. NetScaler Gateway se comunica con StoreFront para proteger las aplicaciones y los datos que entregan Citrix Virtual Apps and Desktops. Los dispositivos de usuario ejecutan la aplicación Citrix Workspace para crear una conexión segura y acceder a las aplicaciones, los escritorios y los archivos.

Los usuarios inician sesiones y se autentican mediante NetScaler Gateway. NetScaler Gateway se implementa y se protege en la zona DMZ. Se configura la autenticación de dos factores. En función de sus credenciales de usuario, los usuarios reciben los recursos y las aplicaciones que les corresponden. Las aplicaciones y los datos se encuentran en los servidores adecuados (no aparecen en el diagrama). Se utilizan servidores independientes para los datos y las aplicaciones confidenciales de seguridad.

Implementación con Citrix Endpoint Management, Citrix Virtual Apps y escritorio

January 26, 2024

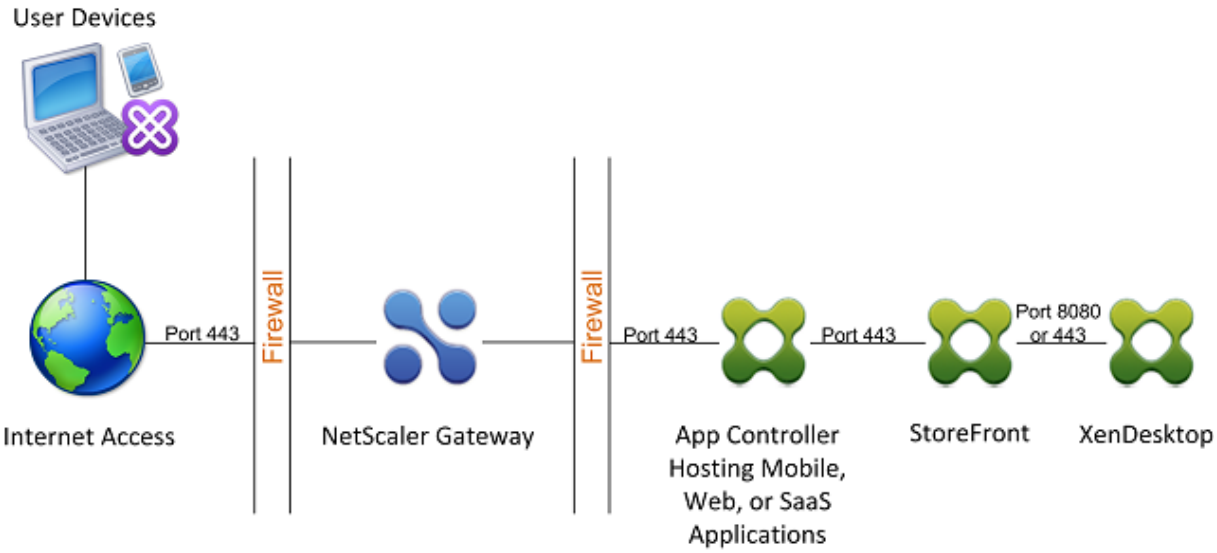
Puede hacer que los usuarios se conecten a aplicaciones Windows, web, SaaS y móviles y escritorios virtuales alojados en su red. Puede proporcionar acceso a sus aplicaciones y escritorios a usuarios remotos e internos mediante NetScaler Gateway, Citrix Endpoint Management y Citrix Virtual Apps and Desktops. NetScaler Gateway autentica a los usuarios y, a continuación, les permite acceder a sus aplicaciones mediante la aplicación Citrix Workspace o Secure Hub.

Los usuarios se conectan a sus aplicaciones basadas en Windows publicadas en Citrix Virtual Apps y escritorios virtuales publicados en Citrix Virtual Desktops mediante la aplicación Citrix Workspace y StoreFront.

Citrix Endpoint Management contiene Citrix Endpoint Management, que permite a los usuarios conectarse a aplicaciones web, SaaS y MDX. Endpoint Management le permite administrar aplicaciones web, SaaS y MDX para el inicio de sesión único (SSO), junto con documentos de ShareFile. Instala Endpoint Management en la red interna. Los usuarios remotos se conectan a Endpoint Management a través de NetScaler Gateway para acceder a sus aplicaciones y datos de ShareFile Los usuarios remotos pueden conectarse con el cliente Citrix Secure Access, la aplicación Citrix Workspace o Secure Hub para acceder a las aplicaciones y a ShareFile. Los usuarios que se encuentran en la red interna pueden conectarse directamente a Endpoint Management mediante la aplicación Citrix Workspace. En la siguiente ilustración se muestra NetScaler Gateway implementado con Endpoint Management y StoreFront.

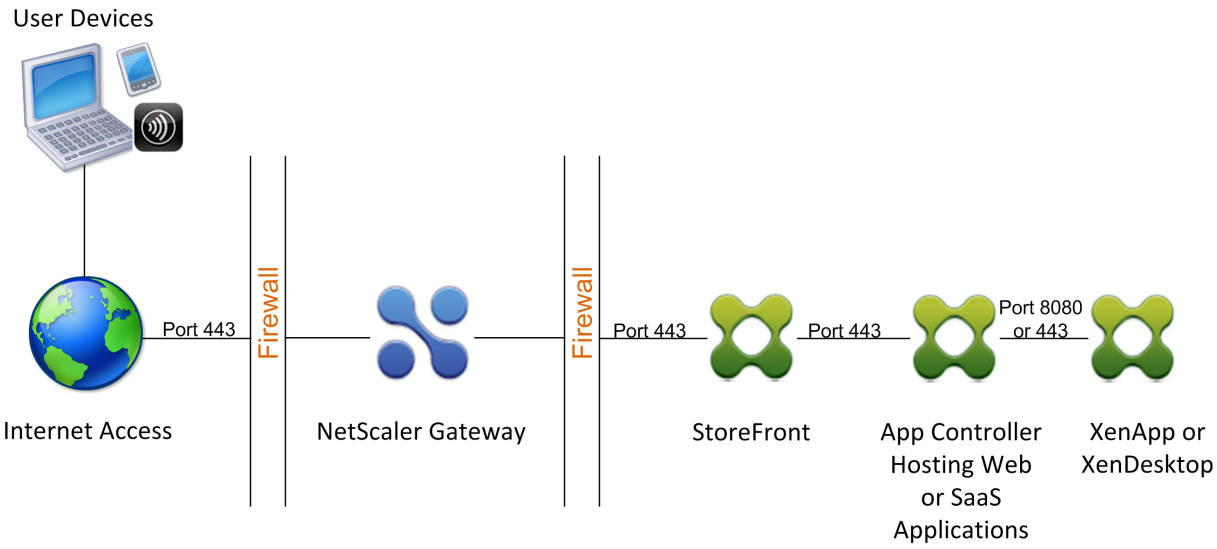
Si su implementación proporciona acceso a aplicaciones MDX desde Endpoint Management y acceso a aplicaciones basadas en Windows desde StoreFront, implemente Endpoint Management delante de StoreFront, como se muestra en la siguiente ilustración:

Figura 1. Implementación de NetScaler Gateway con Endpoint Management en frente de StoreFront



Si la implementación no proporciona acceso a las aplicaciones MDX, StoreFront reside delante de Endpoint Management, como se muestra en la siguiente ilustración:

Figura 2. Implementación de NetScaler Gateway con StoreFront frente a Endpoint Management



Con cada implementación, StoreFront y Endpoint Management deben residir en la red interna y NetScaler Gateway debe estar en la DMZ. Para obtener más información sobre la implementación de Endpoint Management, consulte el tema Instalación de Endpoint Management.
Para obtener más información sobre la implementación de StoreFront, consulte el tema StoreFront.

Configurar parámetros para el entorno de Citrix Endpoint Management

January 26, 2024

El asistente NetScaler para Citrix Endpoint Management le guía a través de la configuración de las funciones de NetScaler para su implementación de Citrix Endpoint Management. Puede utilizar el asistente para:

- **Configure una Micro VPN.** En este caso, los usuarios remotos pueden acceder a aplicaciones y escritorios de la red interna.
  - Para el modo solo MAM de Citrix Endpoint Management, debe usar NetScaler Gateway para la autenticación.
  - Para implementaciones MDM, Citrix recomienda NetScaler Gateway para la VPN de dispositivos móviles.
  - Para implementaciones de ENT, si un usuario opta por no inscribirse en MDM, el dispositivo funciona en el modo MAM heredado y se inscribe mediante el FQDN de NetScaler Gateway.
- **Configure la autenticación basada en certificados.** La configuración predeterminada de Citrix Endpoint Management es la autenticación de nombre de usuario y contraseña. Para agregar otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere la posibilidad de utilizar la autenticación basada en certificados.
- **Equilibrio de carga de servidores Citrix Endpoint Management.** El equilibrio de carga de NetScaler es necesario para todos los modos de dispositivo de Citrix Endpoint Management si tiene varios servidores Citrix Endpoint Management o si Citrix Endpoint Management se encuentra dentro de la red DMZ o interna (y, por lo tanto, el tráfico fluye de los dispositivos a NetScaler a Citrix Endpoint Management). En este escenario, el dispositivo NetScaler reside en la DMZ entre el dispositivo del usuario y los servidores de Citrix Endpoint Management para equilibrar la carga de los datos cifrados enviados desde los dispositivos móviles a los servidores de Citrix Endpoint Management.
- **Equilibrio de carga servidores Microsoft Exchange con filtrado de correo electrónico.** En este caso, el dispositivo NetScaler se encuentra entre el dispositivo de usuario y NetScaler Connector (XNC) de Citrix Endpoint Management y entre el dispositivo de usuario y los servidores CAS de Microsoft Exchange. Todas las solicitudes de los dispositivos de usuario van al dispositivo NetScaler Gateway, que luego se comunica con el XNC para recuperar información sobre el dispositivo. Según la respuesta del XNC, el dispositivo NetScaler reenvía la solicitud desde un dispositivo de la lista de permitidos al servidor de la red interna o interrumpe la conexión desde un dispositivo de la lista de prohibidos.
- **Equilibrio de carga ShareFile StorageZones Connectors basado en el tipo de contenido solicitado.** En este caso se solicita información básica sobre el entorno de Storage Zones Controller y, a continuación, se genera una configuración que hace lo siguiente:
  - Equilibra la carga del tráfico entre los controladores de zonas de almacenamiento.
  - Proporciona autenticación de usuario para los conectores StorageZones.

- Valida las firmas URI para las cargas y descargas de ShareFile.
- Termina las conexiones SSL en el dispositivo NetScaler.

Para obtener más información sobre cómo configurar ShareFile, consulte Configurar NetScaler para Storage Zones Controller.

> **Importante:**
>
> Antes de utilizar el asistente de Citrix Endpoint Management, consulte estos artículos de Citrix Endpoint Management Deployment para obtener información y recomendaciones sobre diseño e implementación:
>
> Integración de Citrix Endpoint Management
>
> Integración en NetScaler Gateway y NetScaler
>
> Consideraciones sobre SSO y proxies para aplicaciones MDX
>
> Autenticación
>
> Puede utilizar NetScaler for Citrix Endpoint Management Wizard solo una vez. Si quiere varias instancias de Citrix Endpoint Management, por ejemplo, para entornos de prueba, desarrollo y producción, debe configurar NetScaler para los entornos adicionales de forma manual. En los siguientes artículos de soporte se enumeran los comandos que ejecuta el asistente y se proporcionan instrucciones para ejecutarlos para crear una instancia de NetScaler:
>
> Comandos generados por Citrix Endpoint Management Wizard en NetScaler - SSL Bridge
>
> Comandos generados por Citrix Endpoint Management Wizard en NetScaler - Descarga SSL

Requisitos de licencia para las funciones de NetScaler

Debe instalar licencias para habilitar las siguientes funciones de NetScaler:

- El equilibrio de carga de MDM de Citrix Endpoint Management requiere una licencia estándar de NetScaler.
- El equilibrio de carga de ShareFile con StorageZones requiere una licencia estándar de NetScaler.
- El equilibrio de carga de Exchange requiere una licencia de NetScaler o una licencia avanzada con la adición de una licencia de almacenamiento en caché integrado.

Asistente de NetScaler para Citrix Endpoint Management

En esta sección se proporciona un ejemplo del uso del asistente NetScaler para Citrix Endpoint Management para:

- Configurar el acceso micro VPN para conexiones de usuarios remotos a los recursos administrados por Citrix Endpoint Management en su red interna
- Configure la autenticación basada en certificados. Para obtener información sobre cómo obtener e instalar un certificado SSL público, consulte Instalación y administración de certificados.
- Configurar el equilibrio de carga para los servidores Citrix Endpoint Management.

Para utilizar el asistente:

1. En la GUI de NetScaler, haga clic en la ficha **Configuración** y, a continuación, haga clic en **XenMobile** en la sección **Integrar con productos Citrix**.
2. Seleccione su versión de Citrix Endpoint Management y, a continuación, haga clic en **Comenzar**.
3. Seleccione las funciones que desea configurar. Puede utilizar este asistente solo una vez, por lo que debe realizar la configuración posterior de forma manual. En estas instrucciones se presupone que debe seleccionar los siguientes ajustes: **Acceso a través de NetScaler Gateway** (para Citrix Endpoint Management que se ejecuta en los modos ENT o MAM) y **Equilibrio de carga de los servidores Citrix Endpoint Management**.
4. En la página **Configuración de NetScaler Gateway**, introduzca los valores de la dirección IP, el puerto y el nombre del servidor virtual de NetScaler Gateway externos.
5. En la página **Certificado de servidor para NetScaler Gateway**, en **Archivo de certificado**, elija el archivo de certificado de **Local** o **Dispositivo**.

    - Local: Seleccione el certificado en su equipo
    - Dispositivo: seleccione el certificado en NetScaler Gateway (dispositivo).

6. En la página **Autenticación**, en **Método de autenticación principal**, seleccione **Certificado de cliente** y, a continuación, introduzca un nombre para el perfil del certificado.

    El siguiente procedimiento presupone que ya dispone de una directiva de certificados.

    Si debe crear una directiva de certificados, haga clic en crear una directiva de certificados. En la pantalla del certificado de Citrix Endpoint Management, elija un certificado de servidor existente o instale uno nuevo. Si ejecuta varios servidores Citrix Endpoint Management, agregue un certificado para cada uno. Para el atributo de nombre de inicio de sesión del servidor, especifique userPrincipalName o sAMAccountName, según sus requisitos.
7. Haga clic en **Dos factores** para habilitar la autenticación de dos factores, la autenticación de certificados de cliente seguida de LDAP o RADIUS como tipo de autenticación secundario.
8. En **Método de autenticación secundario**, seleccione el método de autenticación secundario.

    - Con el certificado de cliente como tipo de autenticación principal, tiene la opción de configurar LDPA (o RADIUS) como tipo de autenticación secundaria.

Para utilizar solo autenticación de certificados de cliente, deje **Segundo método de autenticación** como **Ninguno** y, a continuación, haga clic en **Continuar**.

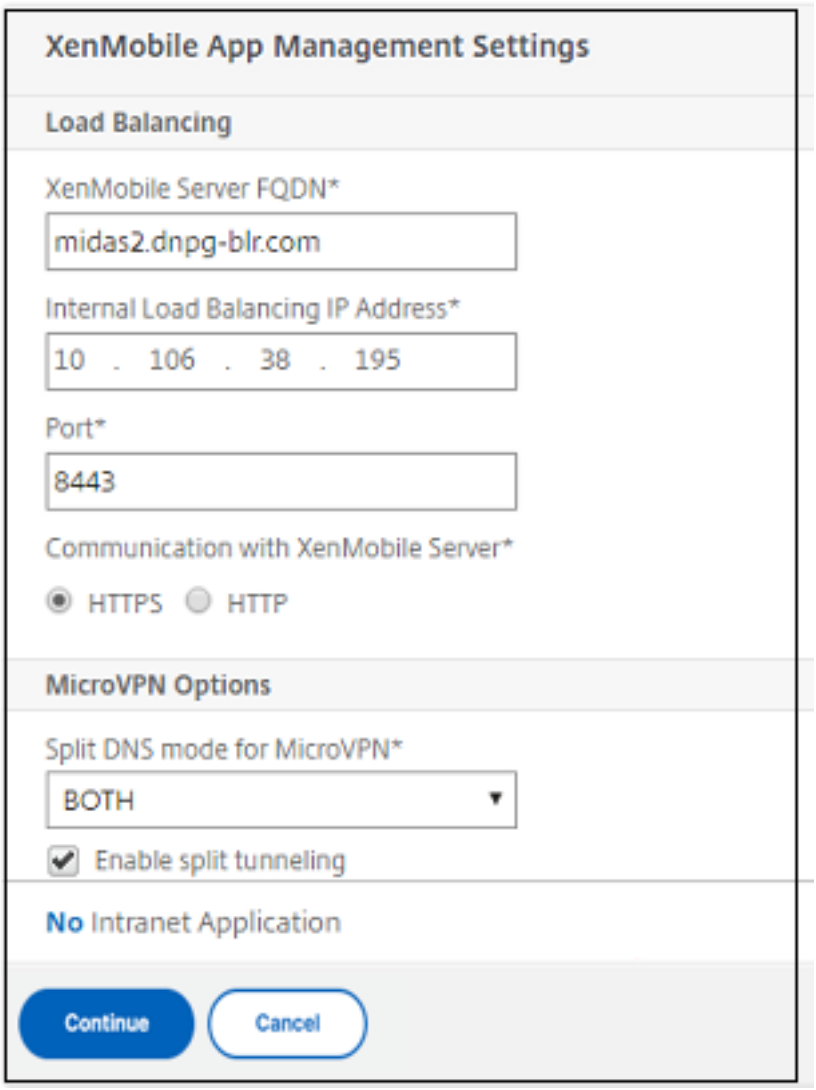
Para usar la autenticación con certificado de cliente y dominio (LDAP), cambie el **método de autenticación secundaria** a **LDAP** y configure los ajustes del servidor de autenticación.

9. Configure la configuración de **administración de aplicaciones Citrix Endpoint Management**.

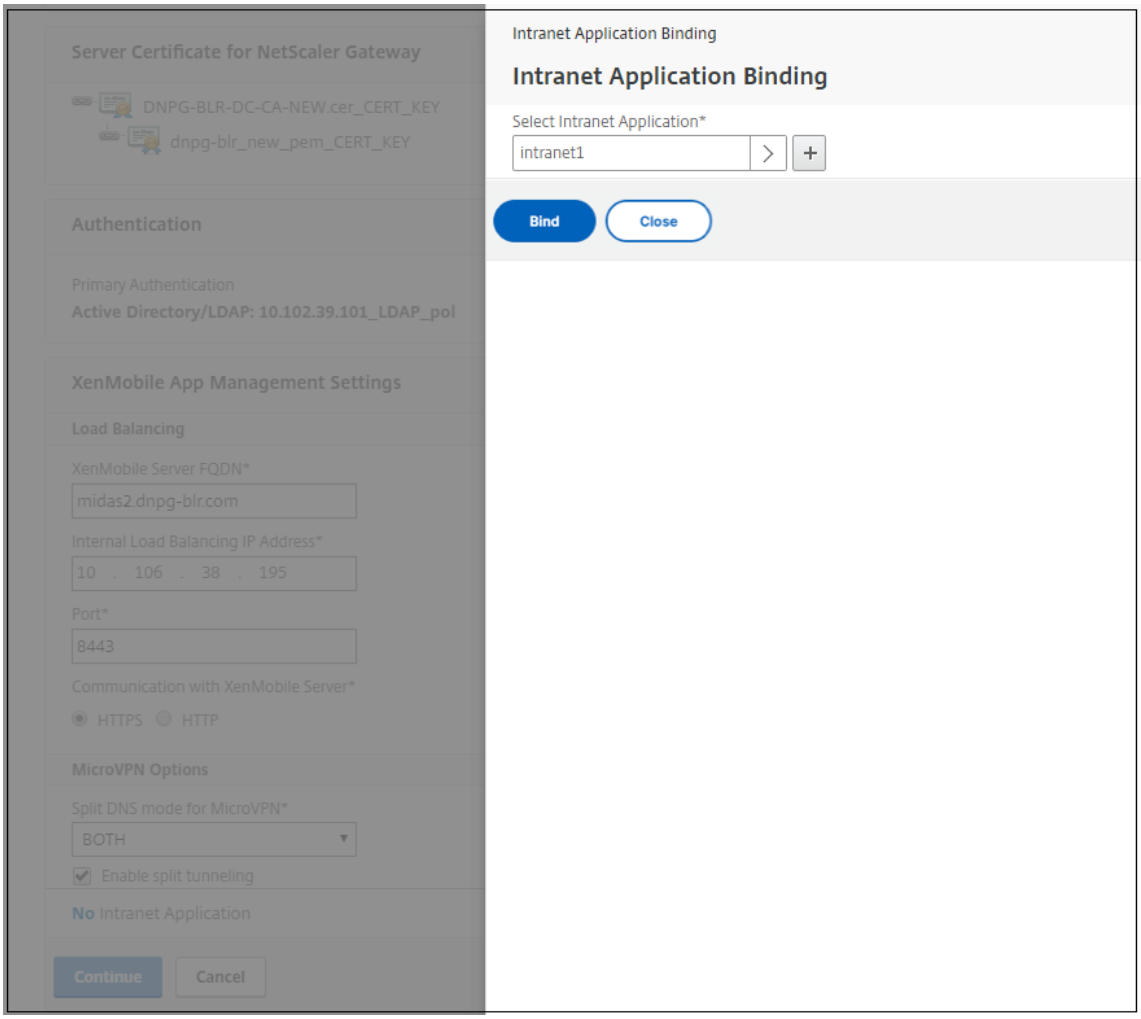
   - Introduzca el **FQDN de Citrix Endpoint Management**. Este es el FQDN de equilibrio de carga para MAM.
   - Introduzca una **dirección IP de equilibrio de carga interna solo para MAM** para el servidor virtual que equilibra la carga de los servidores Citrix Endpoint Management. NetScaler Gateway se comunica con Citrix Endpoint Management a través de esta IP virtual de equilibrio de carga de MAM.
   - Se trata de una implementación de descarga SSL, por lo que seleccione **HTTP** en **Comunicación con Citrix Endpoint Management Server**.
   - El **modo DNS dividido para el campo MicroVPN** se establece automáticamente en **AMBOS**.

   Si su implementación requiere túneles divididos, seleccione **Habilitar túnel dividido**. Configure el enlace de aplicaciones de intranet, a continuación, si habilita la tunelización dividida.

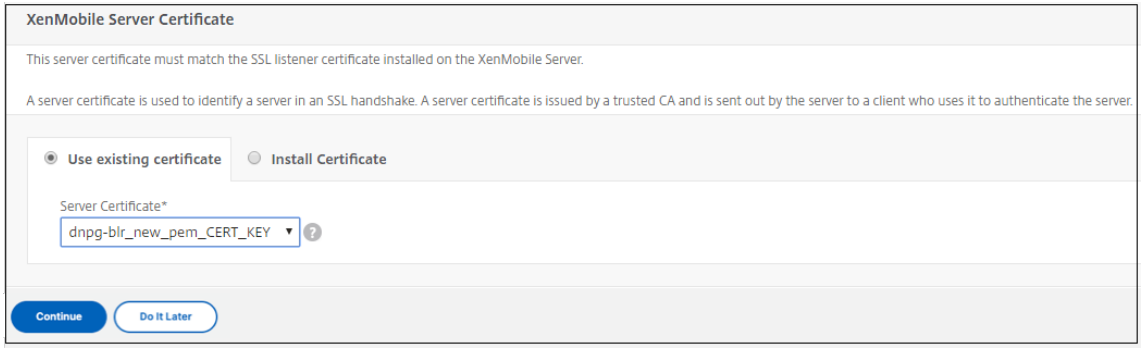
   De forma predeterminada, el acceso Secure Web se tuneliza a la red interna, lo que significa que Secure Web utiliza un túnel VPN por aplicación de vuelta a la red interna para todos los accesos a la red y el dispositivo NetScaler utiliza la configuración del túnel dividido.



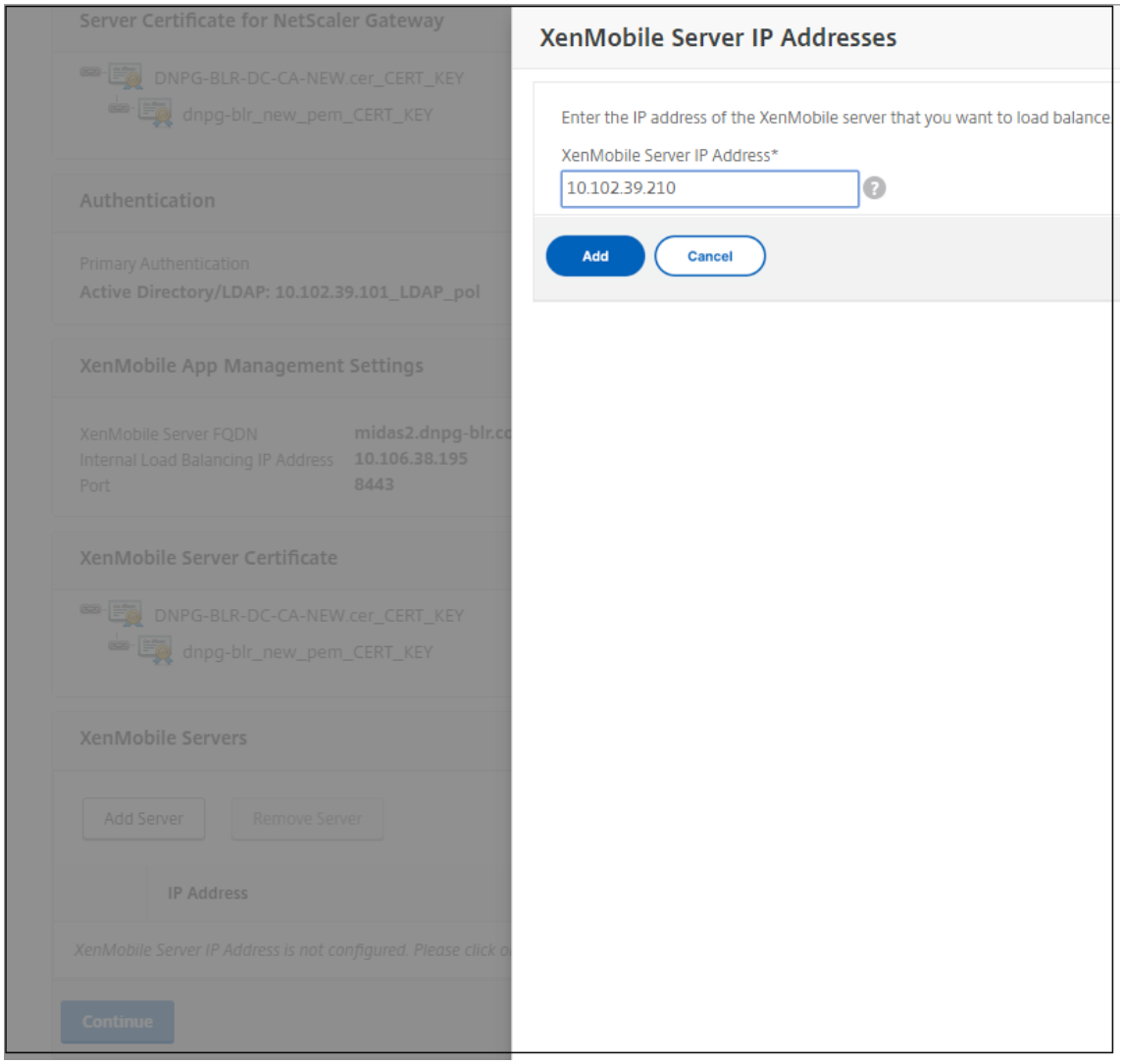
10. Para configurar reglas de interceptación para las conexiones de usuario en NetScaler Gateway, debe configurar el **enlace de aplicaciones de intranet**. Haga clic en **+** para agregar un enlace.



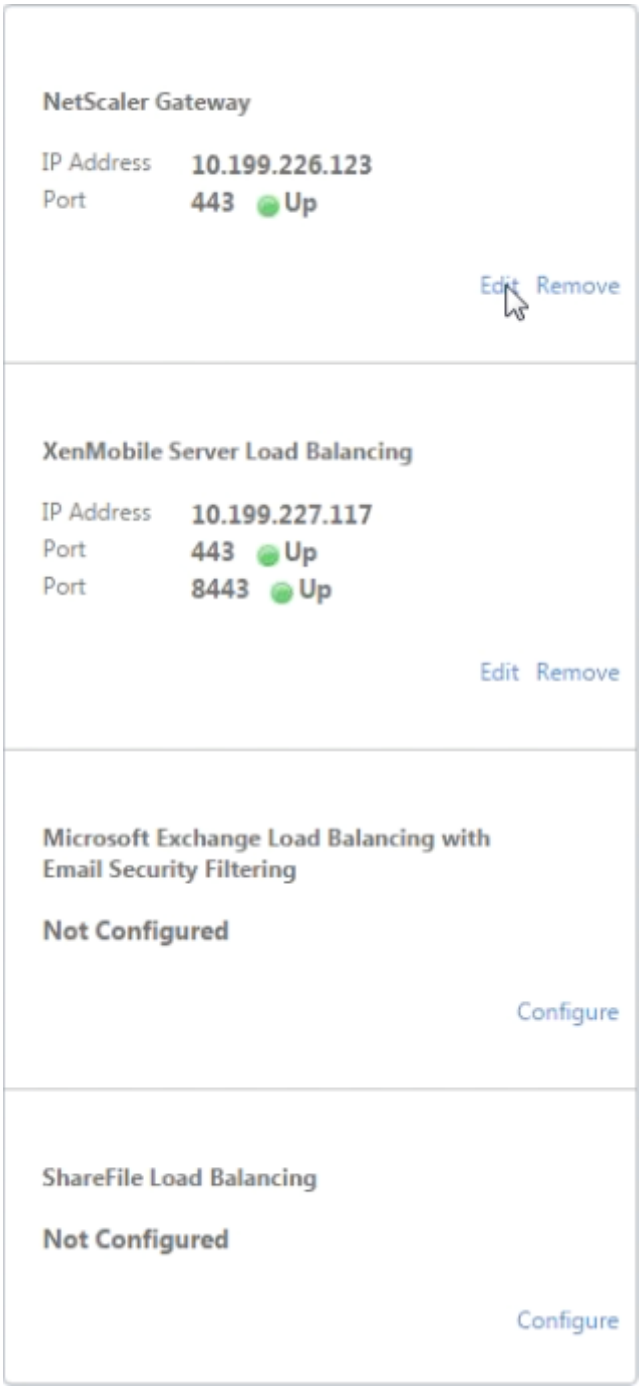
11. Complete los parámetros para permitir el acceso a la red y haga clic en **Crear**.
12. Agregue el certificado de Citrix Endpoint Management. Se utiliza para el servidor virtual de equilibrio de carga de MAM.



13. En **Servidores Citrix Endpoint Management**, haga clic en **Agregar servidor** para agregar la **dirección IP de Citrix Endpoint Management**para enlazar a la IP virtual de equilibrio de carga.



En el panel de NetScaler, confirme que el equilibrio de carga de NetScaler Gateway y Citrix Endpoint Management esté configurado.



Si usa los atributos sAMAccount en los certificados de usuario como alternativa al nombre principal de usuario (UPN), configure el perfil del certificado como se describe en Configuración manual de NetScaler Gateway para la autenticación de certificados de cliente.

Configurar servidores de equilibrio de carga para Citrix Endpoint Management o Citrix XenMobile Server

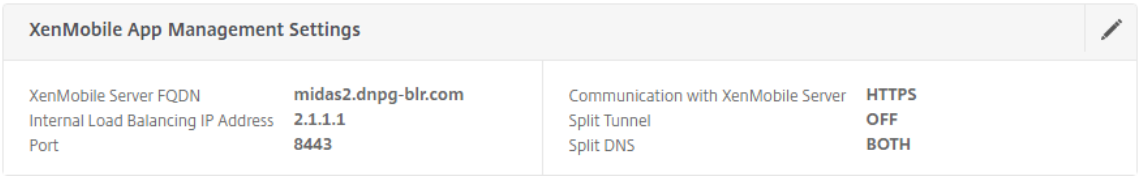
January 26, 2024

Después de utilizar el asistente de **NetScaler para Citrix Endpoint Management** para la configuración inicial, utilice la utilidad de configuración de NetScaler Gateway para configurar el equilibrio de carga, como se describe en esta sección. Para Citrix Endpoint Management, utilice Descarga SSL. Para Citrix Endpoint Management Server, asegúrese de consultar las recomendaciones para los modos de equilibrio de carga en "Resumen de implementación"en Integración con NetScaler Gateway y NetScaler.

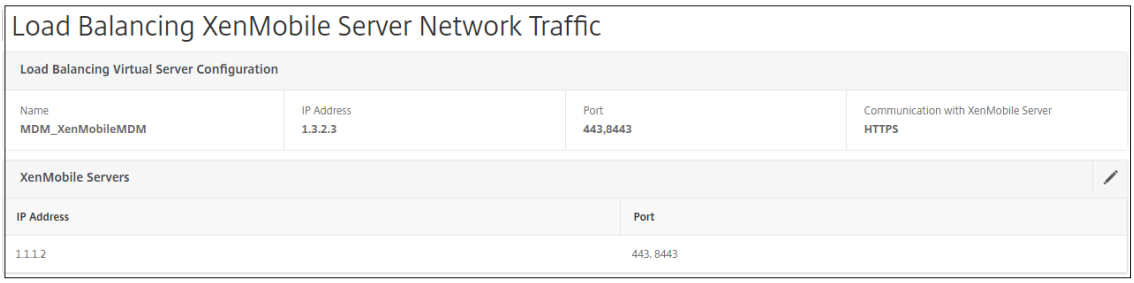
Para usar el modo puente SSL para los VIP de NetScaler

Utilice el modo Puente SSL si Citrix Endpoint Management está en la DMZ. Al equilibrar la carga de Citrix Endpoint Management con VIP de NetScaler en modo Puente SSL, el tráfico de Internet fluye directamente al servidor de Citrix Endpoint Management, donde finalizan las conexiones. El modo Puente SSL es el más simple de configurar. También son más fáciles de solucionar los problemas que causa.

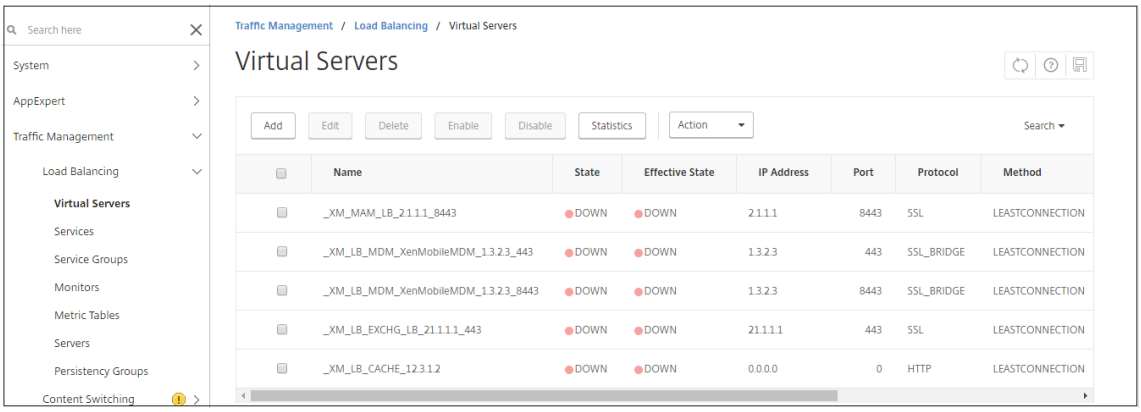
1. Antes de configurar el modo Puente SSL, vaya a **Configuración de administración de aplicaciones Citrix Endpoint Management** y compruebe que **Comunicación con Citrix Endpoint Management Server** es **HTTPS**.



2. Después de iniciar sesión en la utilidad de configuración, en la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
3. En **Servidor virtual LB para administración de dispositivos**, en **Nombre**, escriba un nombre para el servidor.
4. En **Dirección IP**, escriba la dirección IP del servidor virtual y, a continuación, haga clic en **Continuar**.
5. En la página **Equilibrio de carga de Citrix Endpoint Management MDM Servers**, repita los pasos 3 y 4 y, a continuación, haga clic en **Crear**.
6. Compruebe que la configuración sea correcta y, a continuación, haga clic en **Listo**.



7. Para verificar la configuración del equilibrio de carga, vaya a **Administración del tráfico > Servidores virtuales**.



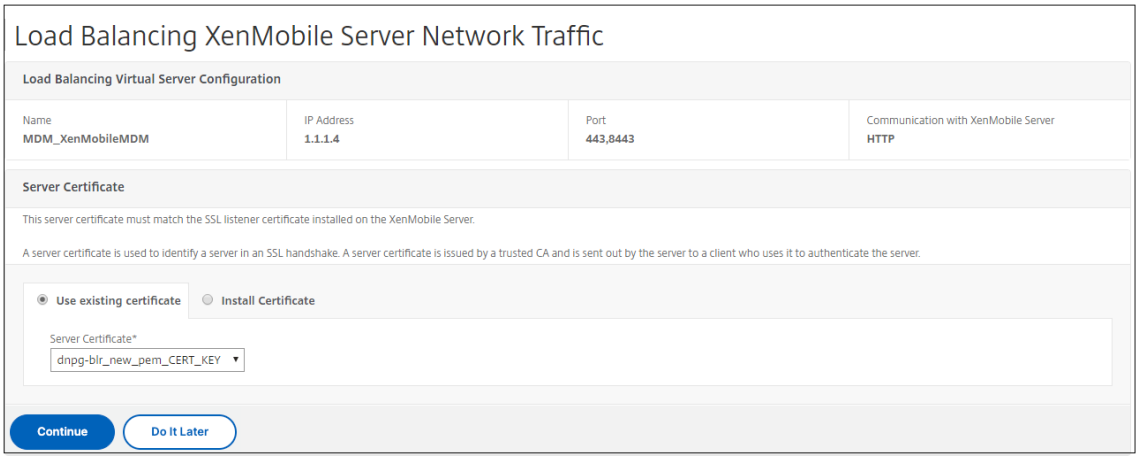
To use SSL Offload mode for NetScaler VIPs

Utilice la descarga de SSL para Citrix Endpoint Management. Utilice también la descarga SSL, si es necesario para cumplir los estándares de seguridad, cuando Citrix Endpoint Management local se encuentre en la red interna. Al equilibrar la carga de Citrix Endpoint Management con VIP de NetScaler en modo Descarga SSL, el tráfico de Internet fluye directamente al dispositivo NetScaler, donde finalizan las conexiones. A continuación, NetScaler Gateway establece nuevas sesiones desde el dispositivo a Citrix Endpoint Management. El modo de descarga SSL implica una mayor complejidad durante la configuración y la solución de problemas.

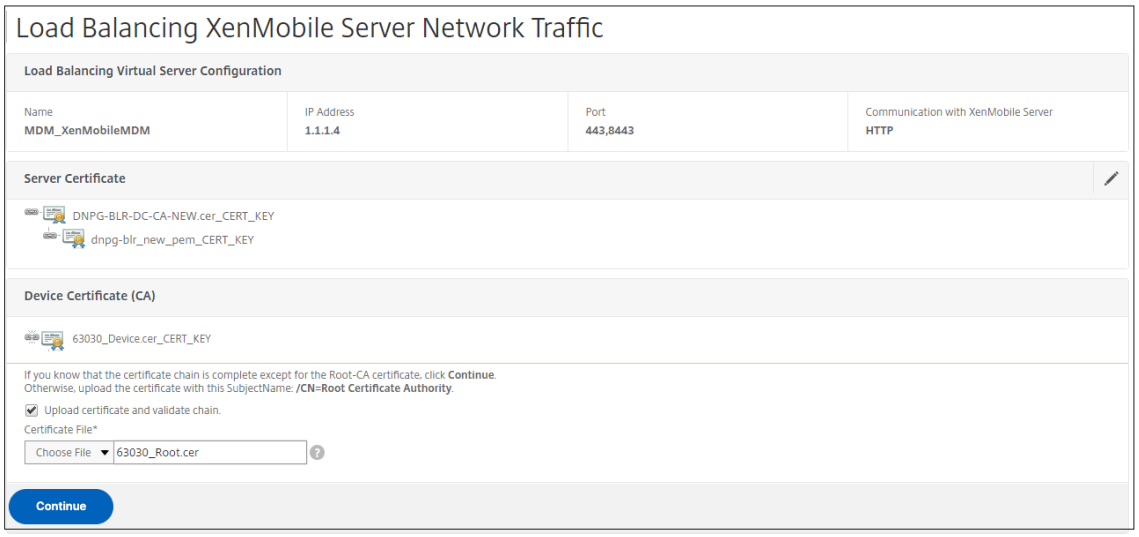
1. Antes de configurar el modo de descarga SSL, vaya a **Citrix Endpoint Management App Management Settings** y compruebe que **Comunicación con Citrix Endpoint Management Server** es **HTTP**.

2. Inicie sesión en la utilidad de configuración. En la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.

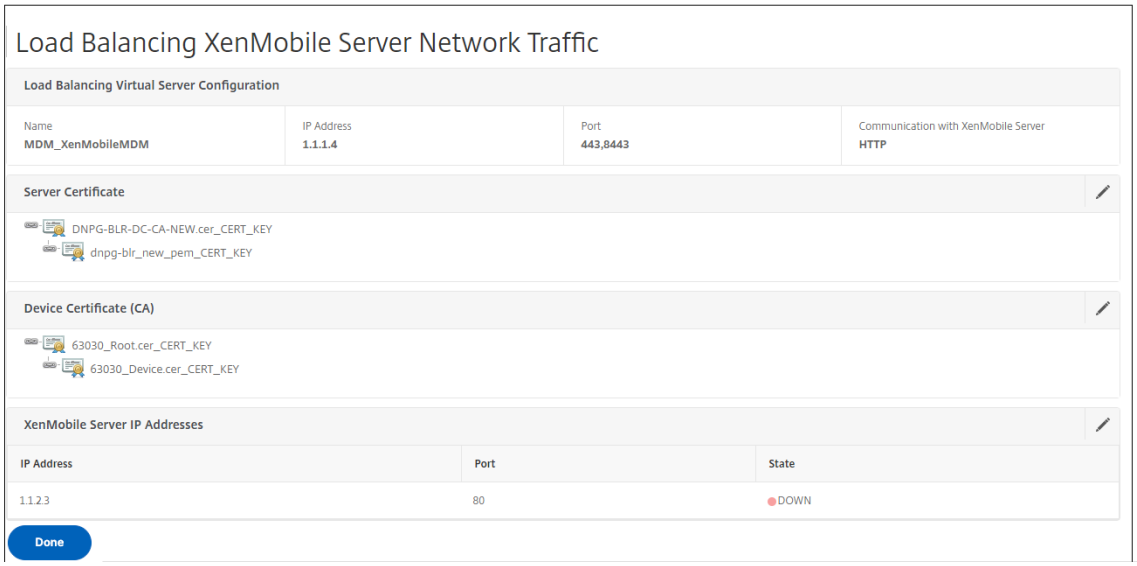
3. En **Servidor virtual LB para administración de dispositivos**, en **Nombre**, escriba un nombre para el servidor.
4. En **Dirección IP**, escriba la dirección IP del servidor virtual y, a continuación, haga clic en **Continuar**.
5. En la página **Equilibrio de carga de Citrix Endpoint Management MDM Servers**, repita los pasos 3 y 4 y, a continuación, haga clic en **Crear**.
6. Compruebe la configuración y, a continuación, haga clic en **Listo**.
7. Cuando se le pida que agregue un certificado de servidor, elija el certificado de servidor y haga clic en **Continuar**.



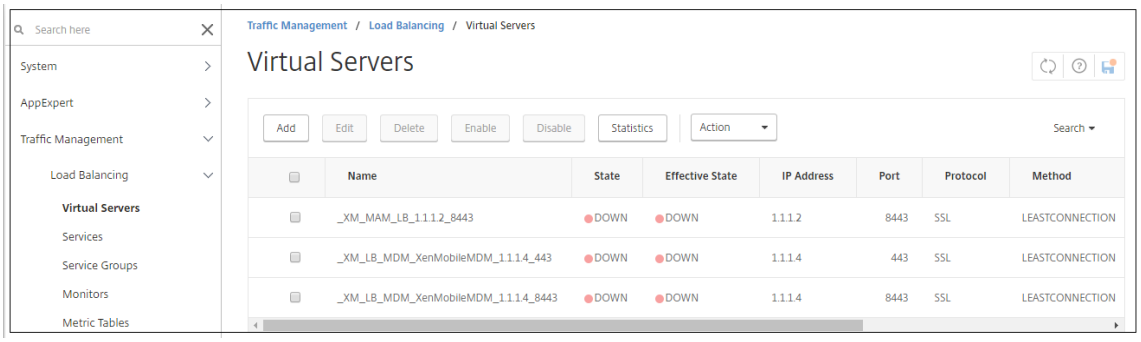
8. Especifique el certificado de CA y haga clic en **Continuar**.



9. Mantenga la misma dirección IP de Citrix Endpoint Management. Haga clic en **Listo**.



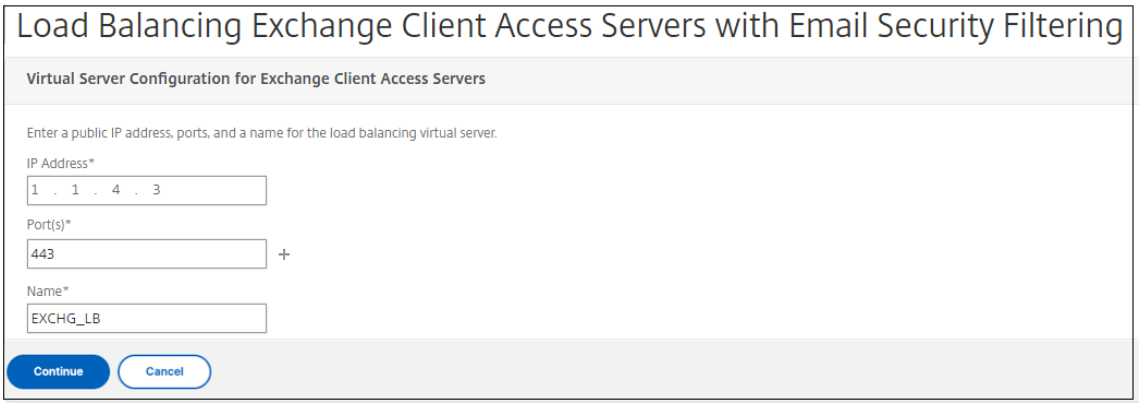
10. Para verificar la configuración del equilibrio de carga, vaya a **Administración del tráfico > Servidores virtuales**.



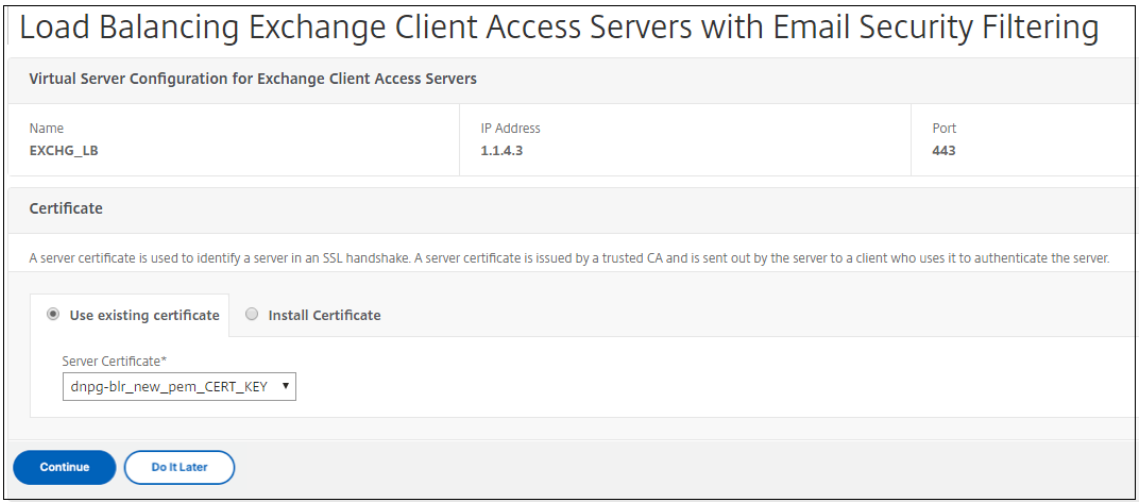
Configurar servidores de equilibrio de carga para Microsoft Exchange con filtrado de seguridad de correo electrónico

January 26, 2024

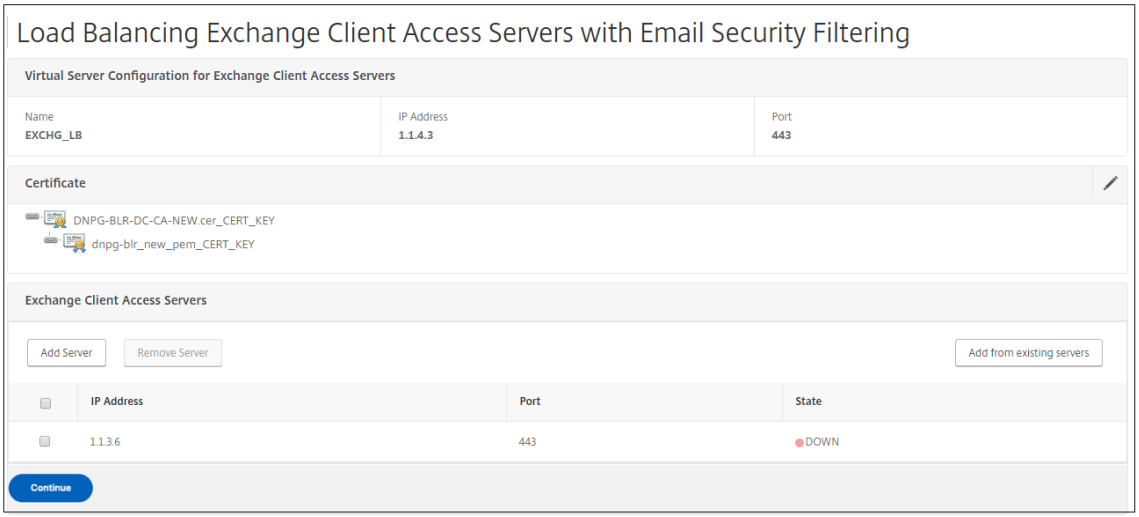
1. En la ficha **Inicio**, en **MDM Server LB**, haga clic en **Configurar**.
2. En **LB Virtual Server for Exchange CAS**, en **Nombre**, escriba un nombre para el servidor.
3. En **Dirección IP**, escriba la dirección IP del servidor virtual.
4. En **Puerto**, escriba el número de puerto. Para agregar más puertos, haga clic en el signo más (**+**) y, a continuación, escriba el número de puerto.
5. Haga clic en **Continuar**.



6. En **Certificados**, elija un certificado existente o instale uno que esté en su equipo (**local**) o en el dispositivo NetScaler (**dispositivo**).
7. Haga clic en **Continuar**.



8. En **Instancias del servicio Citrix Analytics de Exchange**, escriba un nombre, una dirección IP y un número de puerto para el servidor virtual. A continuación, haga clic en **Agregar** y **continuar**.



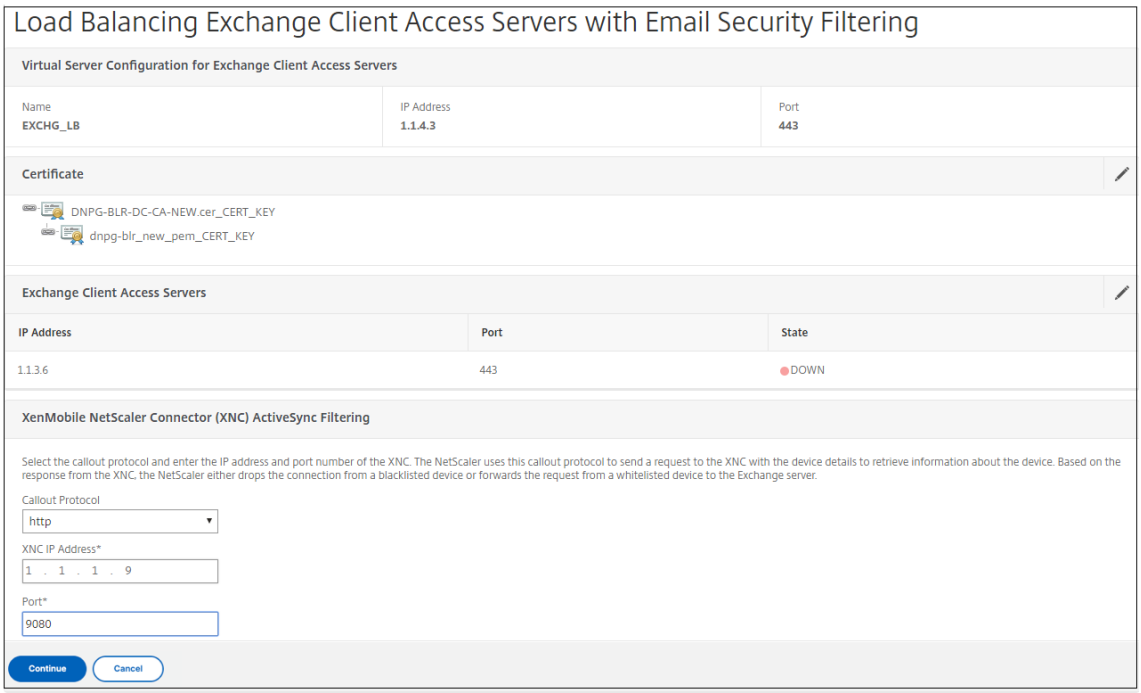
Al **hacer clic en Listo**, aparecen los campos para configurar el filtro ActiveSync de Citrix Endpoint Management de NetScaler Connector (XNC).

Configurar el filtrado ActiveSync de Citrix Endpoint Management NetScaler Connector (XNC)

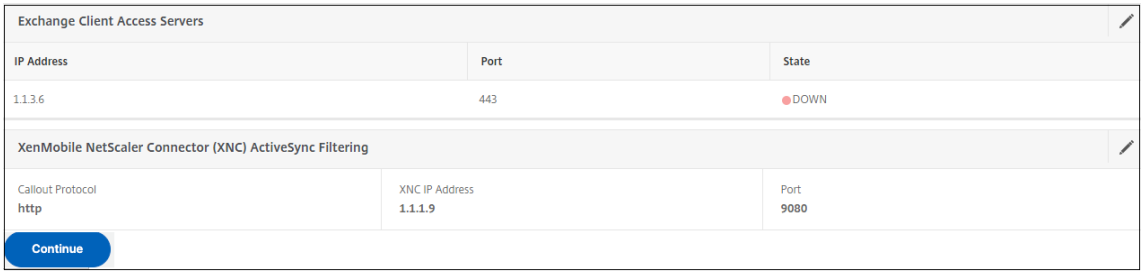
January 26, 2024

Citrix Endpoint Management NetScaler Connector (XNC) proporciona un servicio de autorización a nivel de dispositivo de clientes ActiveSync a NetScaler que actúa como proxy inverso para el protocolo Exchange ActiveSync. La combinación de directivas definidas en Citrix Endpoint Management y reglas definidas localmente por el XNC controla la autorización.

1. En **Filtrado ActiveSync de Citrix Endpoint Management NetScaler Connector (XNC)**, para **Protocolo de llamada**, seleccione **http** o **https**.
2. En **Dirección IP de XNC**, escriba la dirección IP del conector Citrix NetScaler Endpoint Management.
3. En **Puerto**, escriba **9080** para el tráfico de red HTTP o **9443** para el tráfico de red HTTPS y, a continuación, haga clic en **Continuar**.



Aparecerá su configuración.



Permitir el acceso desde dispositivos móviles con Citrix Mobile Productivity Apps

March 27, 2024

El asistente de NetScaler para XenMobile configura la configuración necesaria para permitir a los usuarios conectarse desde dispositivos compatibles a través de NetScaler Gateway a aplicaciones móviles y recursos de la red interna. Los usuarios se conectan mediante Secure Hub (anteriormente, Citrix Secure Hub), que establece un túnel Micro VPN. Cuando los usuarios se conectan, se abre un túnel VPN a NetScaler Gateway y, a continuación, se pasa a XenMobile en la red interna. Los usuarios pueden acceder a sus aplicaciones web, móviles y SaaS desde XenMobile.

Para garantizar que los usuarios consuman una única licencia universal al conectarse a NetScaler Gateway con varios dispositivos simultáneamente, puede habilitar la transferencia de sesiones en el servidor virtual. Para obtener más información, consulte Configuración de tipos de conexión en el servidor virtual.

Si necesita cambiar la configuración después de utilizar el asistente de NetScaler para XenMobile, utilice las secciones de este artículo para obtener orientación. Antes de cambiar la configuración, asegúrese de comprender las implicaciones de los cambios. Para obtener más información, consulte los artículos de XenMobile Deployment.

Configuración de Secure Browse en NetScaler Gateway

Puede cambiar Secure Browse como parte de la configuración global o como parte de un perfil de sesión. Puede enlazar la directiva de sesión a usuarios, grupos o servidores virtuales. Al configurar Secure Browse, también debe habilitar el acceso sin cliente. Sin embargo, el acceso sin cliente no requiere que habilite Secure Browse. Cuando configure el acceso sin cliente, establezca la **codificación URL de acceso sin cliente** en **Borrar**.

Para configurar Secure Browse globalmente:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Seguridad**, haga clic en **Secure Browse** y, a continuación, haga clic en **Aceptar**.

Para configurar Secure Browse en un perfil y directiva de sesión:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, realice una de las acciones siguientes:
   - Si va a crear una nueva directiva de sesión, haga clic en **Agregar**.
   - Si va a cambiar una directiva existente, selecciónela y, a continuación, haga clic en **Abrir**.
3. En la directiva, cree un perfil o modifique un perfil existente. Para hacerlo, realice una de las siguientes acciones:
   - Junto a **Solicitar perfil**, haga clic en **Nuevo**.
   - Junto a **Solicitar perfil** , haz clic en **Modificar** .
4. En la ficha **Seguridad**, junto a **Secure Browse**, haga clic en **Supedición global** y, a continuación, seleccione **Secure Browse**.
5. Lleve a cabo una de las siguientes acciones:
   - Si va a crear un nuevo perfil, haga clic en **Crear**, defina la expresión en el cuadro de diálogo de directivas, haga clic en **Crear y, a continuación,** haga clic en **Cerrar**.
   - Si modifica un perfil existente, después de realizar la selección, haga clic dos veces en **Aceptar**.

Para configurar directivas de tráfico para Secure Web en modo Secure Browse:

Siga estos pasos para configurar las directivas de tráfico para redirigir el tráfico de Secure Web a través de un servidor proxy en modo Secure Browse.

1. En la utilidad de configuración, en la ficha **Configuración**, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Tráfico**.
2. En el panel derecho, haga clic en la ficha **Perfiles de tráfico** y, a continuación, haga clic en **Agregar**.
3. En **Nombre**, introduzca un nombre para el perfil, seleccione **TCP** como **protocolo**y deje el resto de la configuración tal cual.
4. Haga clic en **Crear**.
5. Haga clic en la ficha **Perfiles de tráfico** y, a continuación, haga clic en **Agregar**.

6. En **Nombre**, introduzca un nombre para el perfil y, a continuación, seleccione **HTTP** como **protocolo**.
   Este perfil de tráfico es para HTTP y SSL. El tráfico VPN sin cliente es tráfico HTTP por diseño, independientemente del puerto de destino o del tipo de servicio. Por lo tanto, especifica el tráfico SSL y HTTP como **HTTP** en el perfil de tráfico.
7. En **Proxy**, introduzca la dirección IP del servidor proxy. En **Puerto**, introduzca el número de puerto del servidor proxy.
8. Haga clic en **Crear**.
9. Haga clic en la ficha **Directivas de tráfico** y, después, en **Agregar**.
10. Introduzca el **nombre** de la directiva de tráfico y, para **Solicitar perfil**, seleccione el perfil de tráfico que creó en el paso 3. Escriba la siguiente **expresión** y, a continuación, haga clic en **Crear**:

    ```
    1 REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
        User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
        CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
        Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
        HTTP.URL CONTAINS StoreWeb
    2 <!--NeedCopy-->
    ```

    Esta regla realiza una comprobación basada en el encabezado del host. Para omitir el tráfico de sincronización activa del proxy, sustituya **`ActiveSyncServer`** por el nombre del servidor de sincronización activa adecuado.
11. Haga clic en la ficha **Directivas de tráfico** y, después, en **Agregar**. Introduzca el **nombre** de la directiva de tráfico y, para **Solicitar perfil**, seleccione el perfil de tráfico creado en el paso 6. Escriba la siguiente **expresión** y, a continuación, haga clic en **Crear**:

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

12. Haga clic en la ficha **Directivas de tráfico** y, después, en **Agregar**. Introduzca el **nombre** de la directiva de tráfico y, en **Perfil de solicitud**, seleccione el perfil de tráfico creado en el paso 6. Escriba la siguiente **expresión** y, a continuación, haga clic en **Crear**:

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

13. Vaya a **NetScaler Gateway > Servidores virtuales**, seleccione el servidor virtual en el panel derecho y, a continuación, haga clic en **Modificar**.

14. En la fila **Directivas**, haga clic en **+**.
15. En el menú **Elegir directiva**, seleccione **Tráfico**.
16. Haga clic en **Continuar**.
17. En **Vinculación de directivas**, al lado de **Seleccionar directiva**, haga clic en **>**.
18. Seleccione la directiva que creó en el paso 10 y, a continuación, haga clic en **Aceptar**.
19. Haga clic en **Bind**.
20. En **Directivas**, haga clic en **Directiva de tráfico**.
21. En **Enlace de directivas de tráfico de servidor virtual VPN**, haga clic en **Agregar enlace**.
22. En **Vinculación de directivas**, junto al menú **Seleccionar directiva**, haga clic en **>** para ver la lista de directivas.
23. Seleccione la directiva que creó en el paso 11 y, a continuación, haga clic en **Aceptar**.
24. Haga clic en **Bind**.
25. En **Directivas**, haga clic en **Directivas de tráfico**.
26. En **Enlace de directivas de tráfico de servidor virtual VPN**, haga clic en **Agregar enlace**.
27. En **Vinculación de directivas**, junto al menú **Seleccionar directiva**, haga clic en **>** para ver la lista de directivas.
28. Seleccione la directiva que creó en el paso 12 y, a continuación, haga clic en **Aceptar**.
29. Haga clic en **Bind**.
30. Haga clic en **Cerrar**.
31. Haga clic en **Listo**.

Asegúrese de configurar la aplicación Secure Web (WorxWeb) en la consola de XenMobile. Vaya a **Configurar > Aplicaciones**, seleccione la aplicación Secure Web, haga clic en **Modificar** y, a continuación, realice los siguientes cambios:

- En la página **Información de la aplicación**, cambie el **Modo VPN inicial** a **Secure Browse**.
- En la página **iOS**, cambie el **Modo VPN inicial** a **Secure Browse**.
- En la página **Android**, cambie el **modo VPN preferido** a **Secure Browse**.

Configurar los tiempos de espera de la aplicación y del token MDX

Cuando los usuarios inician sesión desde un dispositivo iOS o Android, se emite un token de aplicación o un token MDX. El token es similar a Secure Ticket Authority (STA).

Puede establecer el número de segundos o minutos que los tokens están activos. Si el token caduca, los usuarios no pueden acceder al recurso solicitado, como una aplicación o una página web.

Los tiempos de espera de los tokens son ajustes globales. Al configurar la configuración, se aplica a todos los usuarios que inician sesión en NetScaler Gateway.

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En el cuadro de diálogo **Configuración global de NetScaler Gateway**, en la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
4. En la ficha **General**, en **Application Token Timeout (seg)** introduzca el número de segundos antes de que caduque el token. El valor predeterminado es de **100** segundos.
5. En Tiempo de **espera del token MDX (minutos)**, introduzca el número de minutos antes de que caduque el token y, a continuación, haga clic en **Aceptar**. El valor predeterminado es de **10** minutos.

Inhabilitar Endpoint Analysis para dispositivos móviles

Si configura el análisis de dispositivos de punto final, debe configurar las expresiones de directiva para que los análisis de análisis de dispositivos de punto final no se ejecuten en dispositivos móviles Android o iOS. Las exploraciones de análisis de dispositivos de punto final no son compatibles con los dispositivos móviles.

Si vincula una directiva de análisis de dispositivos de punto final a un servidor virtual, debe crear un servidor virtual secundario para dispositivos móviles. No vincule las directivas de autenticación previa o posterior a la autenticación al servidor virtual del dispositivo móvil.

Al configurar la expresión de directiva en una directiva de autenticación previa, agrega la cadena User-Agent para excluir Android o iOS. Cuando los usuarios inician sesión desde uno de estos dispositivos y excluye el tipo de dispositivo, el análisis de endpoint no se ejecuta.

Por ejemplo, crea la siguiente expresión de directiva para comprobar si el User-Agent contiene Android, si la aplicación virus.exe no existe y para finalizar el proceso keylogger.exe si se está ejecutando mediante el perfil de autenticación previa. La expresión de directiva podría tener este aspecto:

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

Después de crear la directiva y el perfil de autenticación previa, vincule la directiva al servidor virtual. Cuando los usuarios inician sesión desde un dispositivo Android o iOS, el análisis no se ejecuta. Si los usuarios inician sesión desde un dispositivo basado en Windows, el análisis sí se ejecuta.

Para obtener más información sobre la configuración de directivas de autenticación previa, consulte Configuración de directivas de endpoint.

Admite consultas DNS mediante sufijos DNS para dispositivos Android

Cuando los usuarios establecen una conexión Micro VPN desde un dispositivo Android, NetScaler Gateway envía la configuración de DNS dividida al dispositivo del usuario. NetScaler Gateway admite consultas DNS divididas en función de la configuración de DNS dividida que configure. NetScaler Gateway también admite consultas DNS divididas en función de los sufijos DNS configurados en el dispositivo. Si los usuarios se conectan desde un dispositivo Android, debe configurar la configuración de DNS en NetScaler Gateway.

El DNS dividido funciona de la siguiente manera:

- Si configuras DNS dividido en **Local**, el dispositivo Android envía todas las solicitudes DNS al servidor DNS local.
- Si establece DNS dividido en **Remoto**, todas las solicitudes DNS se envían a los servidores DNS configurados en NetScaler Gateway (servidor DNS remoto) para su resolución.
- Si configuras DNS dividido en **Ambos**, el dispositivo Android comprueba el tipo de solicitud DNS.
  - Si el tipo de solicitud de DNS no es "A", envía el paquete de solicitud de DNS a los servidores DNS locales y remotos.
  - Si el tipo de solicitud de DNS es "A", el complemento de Android extrae el FQDN de la consulta y compara ese FQDN con la lista de sufijos DNS configurada en el dispositivo NetScaler. Si el FQDN de la solicitud de DNS coincide, la solicitud de DNS se envía al servidor DNS remoto. Si el FQDN no coincide, la solicitud DNS se envía a los servidores DNS locales.

En la tabla siguiente se resume el trabajo de DNS dividido según el registro de tipo A y la lista de sufijos.

Configuración DNS dividida	¿Es un disco tipo A?	¿Está en la lista de sufijos?	Dónde se envía la solicitud DNS
Locales	tanto sí como no	tanto sí como no	Locales
Remota	tanto sí como no	tanto sí como no	Remota
Ambos	No	NA	Ambos
Ambos	Sí	Sí	Remota
Ambos	Sí	No	Locales

Para configurar un sufijo DNS:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, seleccione una directiva de sesión y, a continuación, haga clic en **Abrir**.
3. Junto a **Solicitar perfil** , haz clic en **Modificar** .
4. En la ficha **Configuración de red**, haga clic en **Avanzadas**.
5. Junto a **Sufijo DNS de IP de intranet** , haga clic en **Anular global** , escriba el sufijo DNS y, a continuación, haga clic **en**Aceptar tres veces.

Para configurar DNS dividido globalmente en NetScaler Gateway:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway** y, a continuación, haga clic en **Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar la configuración global**.
3. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
4. En la ficha **General**, en **Dividir DNS**, seleccione **Ambos**, **Remoto o**Local**y, a** continuación, haga clic en **Aceptar**.

Para configurar DNS dividido en una directiva de sesión en NetScaler Gateway:

1. En la utilidad de configuración, en la ficha **Configuración**, en el panel de navegación, expanda **NetScaler Gateway > Directivas** y, a continuación, haga clic en **Sesión**.
2. En el panel de detalles, en la ficha **Directivas**, haga clic en **Agregar**.
3. En **Nombre**, escriba un nombre para la directiva.
4. Junto a **Solicitar perfil**, haga clic en **Nuevo**.
5. En **Nombre**, escriba un nombre para el perfil.
6. En la ficha **Experiencia del cliente**, haga clic en **Configuración avanzada**.
7. En la ficha **General**, junto a **Dividir DNS**, haga clic en **Supedición global**, seleccione **Ambos**, **Remoto o**Local**y, a** continuación, haga clic en **Aceptar**.
8. En el cuadro de diálogo **Crear directiva de sesión**, junto a **Expresiones con nombre**, seleccione **General**, **True**, haga clic en **Agregar expresión**, haga clic en **Crear y, a continuación,** haga clic en **Cerrar**.

Configurar la autenticación de dominios y tokens de seguridad para Citrix Endpoint Management

March 27, 2024

Puede configurar Citrix Endpoint Management para exigir a los usuarios que se autentiquen mediante el protocolo RADIUS con sus credenciales de LDAP más una contraseña de un solo uso. En esta sección se describe la configuración necesaria de NetScaler Gateway para ese tipo de autenticación de dos factores.

Requisitos previos

Si aún no ha ejecutado el asistente de NetScaler para Citrix Endpoint Management, consulte la sección Asistente de *NetScaler para Citrix Endpoint Management* en Configuración de las opciones del entorno de Citrix Endpoint Management. Asegúrese de que la configuración de NetScaler incluya lo siguiente:

- **Número de puerto LDAP** = **636** (que es el puerto predeterminado para conexiones LDAP seguras)
- **Atributo de nombre de inicio de sesión del servidor** = **samAccountName** o **userPrincipalName** según sus requisitos

Para configurar la autenticación de dominios y tokens de seguridad

1. Vaya a **NetScaler Gateway > Servidores virtuales**. Seleccione el servidor virtual y, a continuación, haga clic en **Modificar**.
2. Haga clic en **Sin certificado de CA.**
3. En **Seleccionar certificado de CA**, elija un certificado, haga clic en **Aceptar**, en **Enlazar** y, acontinuación, en **Listo**.
4. Vaya a **Directivas > Sesión > Perfiles de sesión**, seleccione el perfil y haga clic en **Modificar**.
5. Haga clic en la ficha **Experiencia del cliente**.
6. En **Índice de credenciales**, elija **SECUNDARIO**.
7. Haga clic en **Aceptar**.
8. Vaya a **Directivas > Autenticación > LDAP**, haga clic en la ficha **Directiva LDAP** y haga clic en **Modificar**.
9. Use la siguiente expresión para usar VIP de NetScaler Gateway independientes para Citrix Endpoint Management y Citrix Virtual Apps and Desktops.

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. Vaya a **Directivas > Autenticación > RADIUS** y, a continuación, haga clic en la ficha **Servidores**.
11. Haga clic en **Agregar**, introduzca los detalles del servidor RADIUS y haga clic en **Crear**.

12. Vaya a **Directivas** y, a continuación, haga clic en **Agregar**.
13. Introduzca un **nombre** para la directiva. En el menú desplegable **Servidor**, seleccione el nombre del servidor RADIUS que ha creado.
14. En **Expresión**, escriba **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver** y haga clic en **Crear**.
15. Seleccione el servidor virtual y, a continuación, haga clic en **Modificar**.
16. En **Autenticación principal**, haga clic en **Directiva LDAP**.
17. Seleccione la directiva, haga clic en **Desvincular**y haga clic en **Cerrar**.
18. En la fila **Autenticación**, haga clic en **+** para agregar la autenticación RADIUS.
19. En **Elegir tipo**, en **Elegir directiva**, seleccione **RADIUS**.
20. Haga clic en **Bind**.
21. Seleccione la directiva de autenticación RADIUS que creó anteriormente y, a continuación, haga clic en **Insertar**.
22. Haga clic en **Aceptar**.
23. Para agregar LDAP como directiva de autenticación secundaria: en la fila **Autenticación**, haga clic en **+**.
24. En **Elegir directiva**, elija **LDAP**.
25. En **Elegir tipo**, elija **Secundaria**.
26. **En Seleccionar directiva**, elija la directiva LDAP.
27. Seleccione la directiva y, a continuación, haga clic en **Aceptar**.
28. Haga clic en **Bind**.
29. Haga clic en **Listo**.
30. Compruebe que las directivas que ha creado tienen la máxima prioridad. Esto garantiza que tengan la máxima prioridad incluso si se agregan más directivas para usuarios que no son móviles. Para obtener más información, consulte Definición de prioridades para directivas de autenticación

Configurar certificado de cliente o certificado de cliente y autenticación de dominio

March 27, 2024

Puede utilizar el asistente de NetScaler para Citrix Endpoint Management para realizar la configuración necesaria para Citrix Endpoint Management al utilizar la autenticación de solo certificado de NetScaler o la autenticación de certificado más dominio. Puede ejecutar el asistente de NetScaler para Citrix Endpoint Management una sola vez. Para obtener información sobre el uso del asistente, consulte Configuración de las opciones del entorno de Citrix Endpoint Management.

Si ya ha utilizado el asistente, siga las instrucciones de este artículo para la configuración adicional necesaria para la autenticación de certificados de cliente o el certificado de cliente más la autenticación de dominio.

Para asegurarse de que el usuario de un dispositivo en modo solo de MAM no puede autenticarse con un certificado existente en el dispositivo, consulte "NetScaler Certificate Revocation List (CRL)"más adelante en este artículo.

Configurar NetScaler Gateway para la autenticación de certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de tipo **SSL** y, en la sección **Parámetros SSL**, establezca **Habilitar reutilización de sesiones** como **INHABILITADO**.
3. Vaya a **NetScaler Gateway**> Servidores virtuales.
4. Seleccione el servidor virtual de tipo **SSL**y haga clic en **Modificar**.
5. En la sección **Parámetros SSL**, haga clic en el icono de modificación.
6. Seleccione **Autenticación de cliente** y en **Certificado de cliente**, seleccione **Obligatorio**.
7. Cree una directiva de certificados de autenticación para que Citrix Endpoint Management pueda extraer el **nombre principal del usuario** o la **cuenta sAMAccount** del certificado de cliente proporcionado por Secure Hub a NetScaler Gateway.
8. Vaya a **NetScaler Gateway > Directivas > Autenticación > CERT**.
9. Haga clic en la ficha **Perfiles** y, a continuación, en **Agregar**.
10. Defina los siguientes parámetros para el perfil del certificado:

    Tipo de autenticación: **CERT**

    Dos factores: **DESACTIVADO** (solo para autenticación con certificado)

    Campo de nombre de usuario: Asunto: **CN**

    Campo de nombre de grupo: **subjectAltName:principalName**
11. Enlazar solo la directiva de autenticación de certificados como **autenticación principal** en el servidor virtual NetScaler Gateway.

12. Enlace el certificado de CA raíz para validar la confianza del certificado de cliente presentado a NetScaler Gateway.

Configurar NetScaler Gateway para la autenticación de dominios y certificados de cliente mediante la interfaz gráfica de usuario

1. Vaya a **Administración del tráfico > Equilibrio de carga > Servidores virtuales**.
2. Seleccione el servidor virtual de tipo **SSL** y, en la sección **Parámetros SSL**, establezca **Habilitar reutilización de sesiones** como **INHABILITADO**.
3. Vaya a **NetScaler Gateway > Directivas > Autenticación > Certificado**.
4. Haga clic en la ficha **Perfiles** y, a continuación, en **Agregar**.
5. Introduzca el **nombre** del perfil, establezca **Two Factoren ON y, enCampo de nombre de usuario**, seleccione **SubjetAltNamePrincipalName**.
6. Haga clic en la ficha **Directivas** y, a continuación, en **Agregar**.
7. Introduzca el **nombre** de la directiva, en **Servidor** seleccione el perfil del certificado, establezca la **expresión** y haga clic en **Crear**.
8. Vaya a **Servidores virtuales**, seleccione el servidor virtual de tipo **SSL**y haga clic en **Modificar**.
9. Junto a **Autenticación**, haga clic en **+** para agregar la autenticación de certificado.
10. Para seleccionar el método de autenticación, en **Elegir directiva**, seleccione **Certificado** y, en **Elegir tipo**, seleccione **Principal**. Esto vincula la autenticación de certificados como autenticación principal con la misma prioridad que el tipo de autenticación LDAP.
11. En **Enlace de directivas**, **haga clic en Haga clic para seleccionar** para seleccionar la directiva de certificados creada anteriormente.
12. Seleccione la directiva de certificados creada anteriormente y haga clic en **Aceptar**.
13. Establezca la **prioridad** en **100** y, a continuación, haga clic en **Vincular**. Utilice el mismo número de prioridad al configurar la directiva de autenticación LDAP en los pasos siguientes.
14. En la fila de **Directiva LDAP**, haga clic en **>**.
15. Seleccione la directiva y, a continuación, en el menú desplegable **Modificar**, haga clic en **Modificar enlace**.
16. Introduzca el mismo valor de **prioridad** que especificó para la directiva de certificados. Haga clic en **Bind**.
17. Haga clic en **Cerrar**.
18. Haga clic en el icono de edición de la sección **Parámetros SSL**.

19. Seleccione la casilla de verificación **Autenticación de cliente** y, en **Certificado de cliente**, elija **Obligatorioy** haga clic en Aceptar.
20. Haga clic en **Listo**.

Lista de revocación de certificados (CRL) de NetScaler

Citrix Endpoint Management admite la lista de revocación de certificados (CRL) solo para una entidad emisora de certificados de terceros. Si tiene configurada una entidad emisora de certificados de Microsoft, Citrix Endpoint Management utiliza NetScaler para administrar la revocación. Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de NetScaler, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse con un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un nuevo certificado porque no impide que un usuario genere un certificado de usuario si se revoca uno. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

Configurar SmartControl

March 27, 2024

SmartControl permite a los administradores definir directivas granulares para configurar y aplicar atributos de entorno de usuario para Citrix Virtual Apps and Desktops en NetScaler Gateway. SmartControl permite a los administradores administrar estas directivas desde una única ubicación, en lugar de hacerlo en cada instancia de estos tipos de servidores.

SmartControl se implementa mediante directivas ICA en NetScaler Gateway. Cada directiva ICA es una combinación de perfiles de expresión y acceso que se puede aplicar a usuarios, grupos, servidores virtuales y de forma global. Las directivas ICA se evalúan después de que el usuario se autentica en el establecimiento de la sesión. Para habilitar SmartControl, debe asociar la directiva ICA a un servidor virtual de VPN.

En la tabla siguiente se enumeran los atributos del entorno de usuario que SmartControl puede aplicar:

ConnectClientDrives	Especifica la conexión predeterminada a las unidades cliente cuando el usuario inicie sesión.

ConnectClientLPTPorts	Especifica la conexión automática de los puertos LPT desde el cliente cuando el usuario inicie sesión. Los puertos LPT son los puertos de impresora local.
ClientAudioRedirection	Especifica las aplicaciones alojadas en el servidor para transmitir audio a través de un dispositivo de sonido instalado en el equipo cliente.
ClientClipboardRedirection	Especifica y configura el acceso al portapapeles en el dispositivo cliente y asigna el portapapeles en el servidor.
ClientCOMPortRedirection	Especifica la redirección del puerto COM hacia y desde el cliente. Los puertos COM son los puertos de comunicación. Los puertos COM son puertos serie.
ClientDriveRedirection	Especifica la redirección de unidades hacia y desde el cliente.
Multistream	Especifica la función multistream para los usuarios especificados.
ClientUSBDeviceRedirection	Especifica la redirección de dispositivos USB hacia y desde el cliente (solo hosts de estación de trabajo).
`Localremotedata`	Especifica la capacidad de descarga de carga de archivos HTML5 para la aplicación Citrix Workspace.
ClientPrinterRedirection	Especifica las impresoras cliente que se asignarán a un servidor cuando un usuario inicie sesión en una sesión.
ClientTWAINDeviceRedirection	Permite el acceso predeterminado o desactiva los dispositivos TWAIN, como cámaras digitales o escáneres, en el dispositivo cliente desde las aplicaciones de procesamiento de imágenes publicadas.
WIARedirection	Permite el acceso predeterminado o inhabilita la redirección del escáner WIA.
DragAndDrop	Permite el acceso predeterminado o desactiva la función de arrastrar y soltar entre aplicaciones y escritorios remotos y del cliente.
SmartCardRedirection	Permita el acceso predeterminado o inhabilite la redirección de tarjetas inteligentes. El canal virtual de tarjetas inteligentes siempre está permitido en CVAD.
FIDO2Redirection	Permite el acceso predeterminado o inhabilita la redirección FIDO2.
Directivas	Acción	Perfiles de acceso
Agregar	Modificar	Eliminar
Mostrar vinculaciones	Administrador de directivas	Acción

Directivas y perfiles de ICA

Directiva de ICA

Una directiva ICA especifica una acción, un perfil de acceso, una expresión y, opcionalmente, una acción de registro. Puede realizar las siguientes configuraciones de directivas ICA:

Configurar una directiva ICA mediante la GUI

1. **Vaya a**NetScaler Gateway > Directivas**y haga clic en ICA.**
2. En la sección **Directivas ICA**, haga clic en **Agregar**. Aparece la página **Crear directiva ICA** .

3. En el campo **Nombre**, especifique un nombre para la directiva ICA.
4. Junto al campo **Acción**, realice una de las siguientes acciones:
    - Haga clic en el icono **>** para seleccionar una acción existente.
    - Haga clic en **Agregar** para crear una acción.
5. Agregue una expresión.
6. Crea una acción de registro.
7. Configure los parámetros restantes según sea necesario y haga clic en **Aceptar**.

Configurar una directiva ICA mediante la CLI `add ica policy smartaccess_policy -rule TRUE -action smartaccess_action`

Enlazar la directiva ICA a un punto de enlace mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > NetScaler Gateway > Directivas y perfiles de ICA > Directivas de ICA**. Haga clic en **Administrador de directivas**.
2. Seleccione el punto de enlace y el servidor virtual y haga clic en **Continuar**.
3. En la sección **Vinculación de directivas**, seleccione la directiva ICA que necesita asociar a un punto de enlace.
4. Haga clic en **Enlazar** y, a continuación, en **Listo**.

Para verificar el enlace, haga clic en **Mostrar enlaces** en la sección **Directivas ICA** . Puede ver la lista de puntos de enlace asociados a la directiva ICA.

Enlazar la directiva ICA a un servidor virtual de VPN mediante la CLI `bind vpn vserver vpnvserver -policy smartaccess_policy -type ICA_REQUEST -priority 10`

Acción de la ICA

Configurar una acción ICA mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas** y, a continuación, haga clic en **ICA**.
2. En la ficha **Acciones ICA**, haga clic en **Agregar**. Aparece la página **Crear acción ICA** .
3. En el campo **Nombre**, especifique un nombre para la directiva ICA.
4. Junto al campo **Perfil de acceso ICA**, realice una de las siguientes acciones:
    - Haga clic en el icono ** para seleccionar un perfil de acceso ICA existente.
    - Haga clic en **Agregar** para crear un perfil de acceso ICA.
5. Cree un perfil de latencia ICA para asociarlo a la acción ICA.
6. Haga clic en **Crear**.

Configurar una acción ICA mediante la CLI `add ica action smartaccess_action -accessProfileName smartaccess_profile`

Perfil de acceso ICA

Un perfil ICA define la configuración de las conexiones de usuario. Los perfiles de acceso especifican las acciones que se aplican al entorno ICA de Citrix Virtual Apps and Desktops and Desktops de un usuario si el dispositivo del usuario cumple las condiciones de expresión de la directiva. Puede utilizar la interfaz gráfica de usuario para crear perfiles ICA por separado de una directiva ICA y, a continuación, utilizarlo para varias directivas. Solo puede utilizar un perfil con una directiva.

Puede crear perfiles de acceso independientes de una directiva ICA. Al crear la directiva, puede seleccionar el perfil de acceso que quiere asociar a la directiva. Un perfil de acceso especifica los recursos disponibles para un usuario.

A partir de la versión 14.1-8.x, NetScaler Gateway amplía las capacidades de la función SmartControl a más canales virtuales ICA de Citrix Virtual Apps and Desktops. Esta extensión mejora la interacción entre NetScaler Gateway y los canales virtuales ICA.

Para aprovechar la capacidad de la función SmartControl ampliada, puede configurar los siguientes ajustes en el perfil de acceso ICA.

- ClientTWAINDeviceRedirection
- WIARedirection
- DragAndDrop
- SmartCardRedirection
- FIDO2Redirection

Configurar un perfil de acceso ICA mediante la GUI

1. **Vaya a**NetScaler Gateway > Directivas > Directivas y perfiles ICA de NetScaler Gateway > Perfiles de acceso y**haga clic en Agregar.** Aparece la página **Crear perfil de acceso ICA** .
2. Proporcione un nombre para el perfil de acceso ICA, configure los siguientes parámetros y haga clic en **Crear**.

    - Conectar los puertos LPT del cliente: permite o bloquea la conexión automática de los puertos del terminal de impresión de línea (LPT) desde el cliente cuando el usuario inicie sesión.
    - Redirección de audio del cliente: permite o bloquea las aplicaciones alojadas en un servidor para reproducir sonidos a través de un dispositivo de sonido instalado en el equipo cliente. Esta configuración también permite o impide que los usuarios graben entradas de audio.

- Intercambio de datos remoto local: permita o bloquee el intercambio de archivos o datos a través de la aplicación Citrix Workspace para HTML5.
- Redirección del portapapeles del cliente: permite o bloquea el portapapeles del dispositivo cliente para que se asigne al portapapeles del servidor.
- Redirección de puertos COM del cliente: permite o bloquea la redirección de puertos de comunicación (COM) hacia y desde el cliente.
- Redirección de unidades de cliente: permite o bloquea la redirección de unidades hacia y desde el cliente.
- Redirección de impresoras de clientes: permite o bloquea la asignación de impresoras a un servidor cuando un usuario inicie sesión.
- Transmisión múltiple: permite o bloquea la función de transmisión múltiple para los usuarios especificados.
- Redirección de la unidad USB del cliente: permite o bloquea la redirección de dispositivos USB hacia y desde el cliente.
- Redirección de dispositivos TWAIN del cliente: permite o bloquea los dispositivos TWAIN, como cámaras digitales o escáneres, en el dispositivo cliente desde las aplicaciones de procesamiento de imágenes publicadas.
- Redirección WIA: permite o bloquea la redirección del escáner de adquisición de imágenes de Windows (WIA).
- Arrastrar y soltar: permite o bloquea la acción de arrastrar y soltar entre escritorios y aplicaciones cliente y remotas.
- Redirección de tarjetas inteligentes: permite o bloquea la redirección de tarjetas inteligentes. El canal virtual de tarjetas inteligentes siempre está permitido en Citrix Virtual Apps and Desktops.
- Redirección FIDO2: permite o bloquea las redirecciones de Fast Identity Online 2 (FIDO 2).

Configurar un perfil de acceso ICA mediante la CLI

```
add ica accessprofile <name> [-ConnectClientLPTPorts ( DEFAULT |
    DISABLED )] [-ClientAudioRedirection ( DEFAULT | DISABLED )][-
    LocalRemoteDataSharing ( DEFAULT | DISABLED )][-
    ClientClipboardRedirection ( DEFAULT | DISABLED )][-
    ClientCOMPortRedirection ( DEFAULT | DISABLED )][-
    ClientDriveRedirection ( DEFAULT | DISABLED )][-
    ClientPrinterRedirection ( DEFAULT | DISABLED )] [-Multistream (
    DEFAULT | DISABLED )][-ClientUSBDriveRedirection ( DEFAULT |
    DISABLED)] [-ClientTWAINDeviceRedirection ( DEFAULT | DISABLED )][-
    WIARedirection ( DEFAULT | DISABLED )] [-DragAndDrop ( DEFAULT |
    DISABLED )] [-SmartCardRedirection ( DEFAULT | DISABLED )]
[-FIDO2Redirection ( DEFAULT | DISABLED )]

<!--NeedCopy-->
```


Perfil de latencia ICA

Configurar un perfil de latencia ICA mediante la GUI

1. Vaya a **NetScaler Gateway > Directivas > Directivas y perfiles ICA de NetScaler Gateway > Perfiles de latencia ICA**.
2. Actualice los campos obligatorios y haga clic en **Crear**.

Configurar un perfil de latencia ICA mediante la CLI

```
add ica latencyprofile [-l7LatencyMonitoring ( ENABLED | DISABLED )]
[-l7LatencyThresholdFactor ] [-l7LatencyWaitTime ] [-l7LatencyNotifyInterval
 ] [-l7LatencyMaxNotifyCount ]
```

Integración de Microsoft Intune

January 26, 2024

La integración de Microsoft Intune con NetScaler Gateway proporciona la mejor solución de protección de datos y acceso a aplicaciones de su clase ofrecida por NetScaler Gateway e Intune.

Obtienes el conjunto más completo de aplicaciones de productividad seguras, como correo electrónico, calendario, contactos, toma de notas, modificación de documentos y acceso remoto, todo lo cual se puede administrar de forma centralizada en diferentes plataformas. La integración de Intune y NetScaler Gateway proporciona funcionalidades de administración de dispositivos móviles (MDM) de primera clase, mientras que la tecnología del lado del cliente Citrix Secure Access permite a estas aplicaciones avanzadas de Intune acceder a los datos y las aplicaciones corporativos de forma segura a través de NetScaler Gateway.

La integración permite a NetScaler Gateway extraer datos de cumplimiento de Intune, lo que permite directivas de acceso condicional. Las directivas de acceso condicional proporcionan a NetScaler Gateway un control más preciso sobre la regulación del acceso en función de las funcionalidades del dispositivo, etc. Por ejemplo, un administrador puede crear una directiva en la que solo se conceda acceso a los dispositivos con "Cámara"inhabilitada.

NetScaler Gateway admite la autenticación de tokens de Azure Active Directory Libraries (ADAL) una vez configurado el servidor virtual de NetScaler Gateway. Tras la configuración, una aplicación móvil empaquetada con la envoltura o SDK de Citrix Network-Only accede a NetScaler Gateway mediante un token ADAL que la aplicación puede obtener directamente de AAD.

Integración de micro VPN de Citrix con Microsoft Endpoint Manager

Los clientes de NetScaler Gateway pueden usar micro VPN con Microsoft Endpoint Manager (Intune). La integración de micro VPN de Citrix con Microsoft Endpoint Management permite que sus aplicaciones accedan a los recursos locales.

La tecnología micro VPN de Citrix proporciona una VPN bajo demanda que reduce los costes de transferencia de datos y simplifica la seguridad, ya que el túnel VPN no siempre está activo. En cambio, solo está activo cuando es necesario, lo que reduce el riesgo y optimiza el rendimiento del dispositivo para mejorar la experiencia del usuario. Esto también ayuda a mejorar la duración de la batería del móvil. La tecnología micro VPN de NetScaler proporciona a los usuarios móviles un acceso seguro a los recursos empresariales internos y, al mismo tiempo, les brinda la mejor experiencia de usuario.

Micro VPN solo es compatible con los siguientes casos de uso:

- Solo administración de aplicaciones móviles (MAM) de Intune
- Administración de dispositivos móviles (MDM) de Intune y administración de aplicaciones móviles (MAM)

> **Importante:**
>
> Para la funcionalidad de VPN SSL, la micro VPN requiere una edición NetScaler Gateway Advanced o Premium (VPX 3000 o una versión posterior) y un permiso de Citrix Endpoint Management. El permiso de Citrix Endpoint Management garantiza la compatibilidad continua con el SDK de micro VPN en exploradores web móviles de Microsoft Edge (iOS y Android). Para obtener más información, contacte con su representante de ventas, cuentas o socios.

Para obtener más información sobre cómo configurar la integración de micro VPN de Citrix con Microsoft Endpoint Manager, consulte Configurar NetScaler Gateway para usar micro VPN con Microsoft Endpoint Manager.

Cuándo utilizar la solución MDM integrada de Intune

January 26, 2024

Los siguientes casos ilustran el uso de la solución MDM de Intune integrada:

- Un nuevo cliente decide incorporar Intune con la implementación local de NetScaler Gateway
- Un usuario existente de NetScaler Gateway quiere agregar la administración de dispositivos móviles con Intune
- Un usuario de Intune existente quiere permitir que los dispositivos móviles o las aplicaciones accedan a los datos ubicados dentro de la red de la empresa con un dispositivo físico o virtual de NetScaler Gateway en la DMZ de la empresa

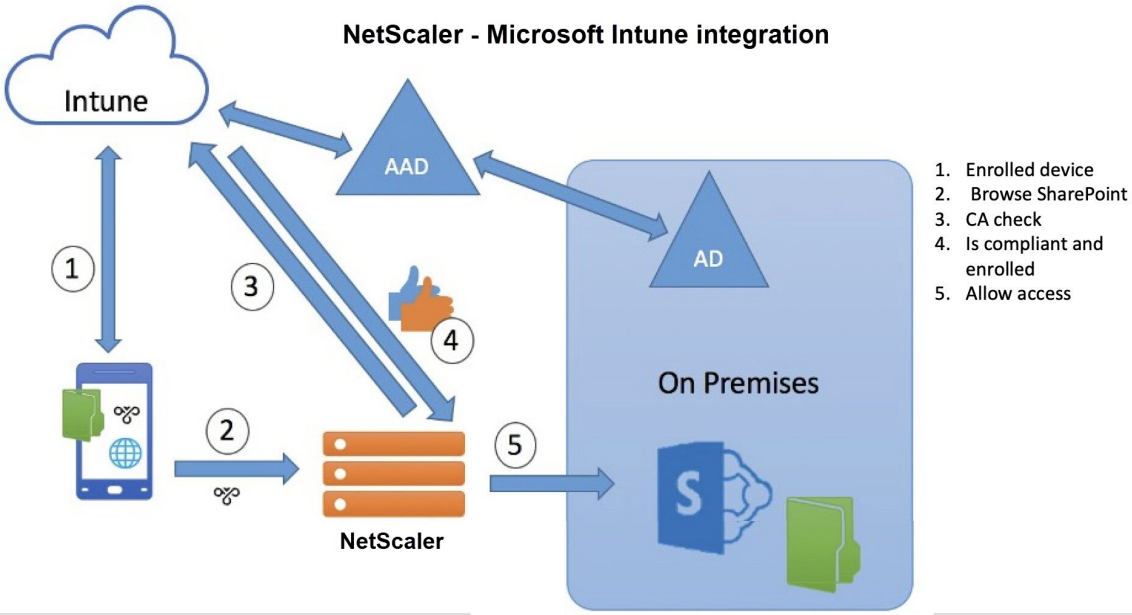
> **Nota**
>
> Solo se admiten clientes iOS y Android.

Descripción de la integración de MDM de NetScaler Gateway con Intune

January 26, 2024

A continuación se muestra un ejemplo de flujo de eventos en una integración de MDM típica de NetScaler Gateway con Intune:

1. Inscribir un dispositivo móvil en Intune.
2. Las directivas de dispositivos y las aplicaciones aprobadas por la empresa se insertan en el dispositivo.
3. Examine SharePoint (aplicación local) desde el dispositivo.
4. La solicitud del explorador va a NetScaler Gateway.
5. El dispositivo NetScaler Gateway comprueba con Intune el estado de inscripción del dispositivo.
6. Si un dispositivo compatible se inscribe correctamente, se concede el acceso a SharePoint.



Cuando un dispositivo no cumple una directiva de acceso condicional, el cliente VPN de NetScaler Gateway muestra un mensaje de error. El mensaje proporciona un enlace desde el dispositivo a una página alojada por Intune que ofrece al usuario la opción de inscribirse o corregir el estado de cumplimiento del dispositivo.

> **Nota:**
>
> Los administradores deben asegurarse de lo siguiente al empujar los certificados a Intune para que los usuarios puedan diferenciar entre los distintos certificados de su dispositivo.

- Los certificados deben tener un resumen de asignaturas.
- Los resúmenes temáticas de los distintos certificados deben ser distintos.

Compatibilidad con la API Intune NAC v2

Como parte de la compatibilidad con la API de Intune NAC v2, debe vincular un archivo de entidad de certificación (certificado de CA) para garantizar que el dispositivo NetScaler obtenga un certificado válido de los dispositivos móviles. En Intune NAC v2, los dispositivos móviles envían ID de dispositivo como parte del certificado de CA. El certificado de CA enlazado aquí debe ser el que se utilice para emitir certificados de cliente para los dispositivos iOS y Android de los usuarios finales. Si hay certificados intermedios, también deben vincularse aquí.

Para obtener más información, consulte Compatibilidad con la API de Intune NAC v2

Configurar comprobación de dispositivo de control de acceso a redes para el servidor virtual de NetScaler Gateway para iniciar sesión en un solo

March 27, 2024

En este tema se proporciona información sobre cómo configurar NetScaler Gateway para conectarse a una red interna desde un dispositivo móvil (iOS y Android) con la seguridad de conformidad de acceso a la red (NAC) que ofrece Microsoft Intune. Cuando un usuario intenta conectarse a NetScaler Gateway desde un cliente VPN para iOS o Android, la puerta de enlace comprueba primero con el servicio Intune si el dispositivo es un dispositivo administrado y que cumple los requisitos.

- Administrado: El dispositivo se inscribe mediante el cliente del portal de empresa de Intune.
- Cumple con los requisitos: se aplican las directivas necesarias enviadas desde el servidor MDM de Intune.

Solo si el dispositivo está administrado y es compatible, se establece la sesión VPN y se proporciona acceso al usuario a los recursos internos.

Nota:

- En esta configuración, NetScaler Gateway en el back-end habla con el servicio Intune. Los perfiles SSL gestionan las conexiones entrantes a NetScaler Gateway. La comunicación back-end de NetScaler Gateway gestiona todos los requisitos de SNI de los servicios en la nube de back-end (Intune).
- El servidor virtual de puerta de enlace SNI para DTLS se admite en NetScaler Gateway versión 13.0 compilación 64.x y posteriores.
- La comprobación de NAC de Intune, para la VPN por aplicación o incluso para la VPN de todo el dispositivo, solo se admite cuando el portal de administración de Intune aprovisiona el perfil de VPN (ahora conocido como Microsoft Endpoint Manager). Estas funciones no son compatibles con los perfiles VPN agregados por el usuario final. El administrador de Intune debe implementar el perfil VPN en su dispositivo desde Microsoft Endpoint Manager para utilizar la comprobación de NAC en el dispositivo del usuario final.

Licencias

Se requiere una licencia de Citrix Enterprise Edition para esta funcionalidad.

Requisitos del sistema

- NetScaler Gateway versión 11.1 compilación 51.21 o posterior
- VPN para iOS: 10.6 o posterior
- VPN para Android: 2.0.13 o posterior
- Microsoft
  - Acceso a Azure AD (con privilegios de arrendatario y administrador)
  - Tenant habilitado para Intune
- Firewall:
  Habilite reglas de firewall para todo el tráfico DNS y SSL desde la dirección IP de subred a `https://login.microsoftonline.com` y `https://graph.windows.net` (puerto 53 y puerto 443)

Requisitos previos

- Todas las directivas de autenticación existentes deben convertirse de directivas clásicas a directivas avanzadas. Para obtener información sobre cómo convertir de directivas clásicas a directivas avanzadas, consulte https://support.citrix.com/article/CTX131024.

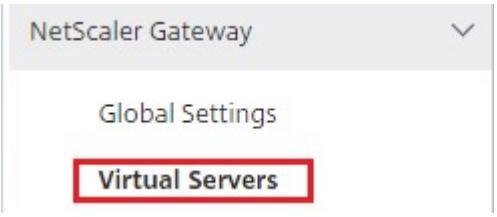
- Cree una aplicación NetScaler Gateway en el portal de Azure. Para obtener más información, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure.
- Configure la directiva OAuth en la aplicación NetScaler Gateway que creó mediante la siguiente información específica de la aplicación.
  - ID de cliente/ ID de aplicación
  - Secreto de cliente/clave de aplicación
  - ID de arrendatario Azure

Referencias

- Este documento captura la configuración de configuración de NetScaler Gateway. La mayor parte de la configuración del cliente de Citrix SSO (iOS/Android) se realiza en el lado de Intune. Para obtener más información sobre la configuración de VPN de Intune para NAC, consulte https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate.
- Para configurar el perfil VPN de una aplicación iOS, consulte https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios.
- Para configurar la aplicación NetScaler Gateway en el portal de Azure, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure.

Para agregar un servidor virtual de NetScaler Gateway con nFactor para la implementación de gateway

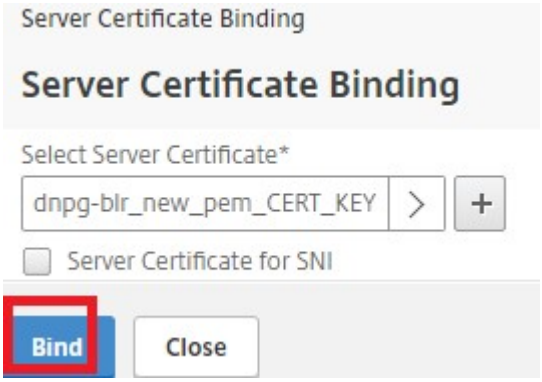
1. Vaya a **NetScaler Gateway**> Servidores virtuales.



2. Haga clic en **Agregar**.
3. Proporcione la información necesaria en el área **Configuración básica** y haga clic en **Aceptar**.

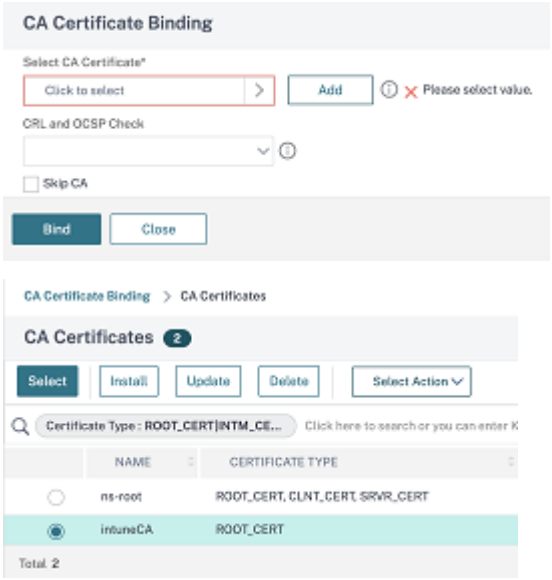
4. Seleccione **Certificado de servidor**.

5. Seleccione el certificado de servidor necesario y haga clic en **Vincular**.



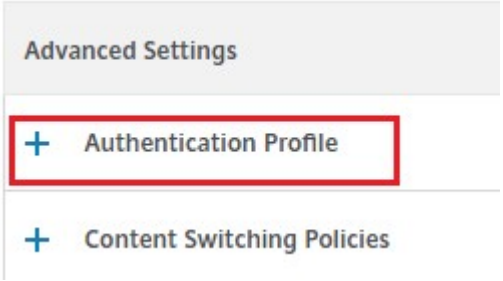
6. Como parte de la compatibilidad con la API de Intune NAC v2, debe vincular un archivo de entidad de certificación (certificado de CA) para garantizar que el dispositivo NetScaler obtenga un certificado válido de los dispositivos móviles. En Intune NAC v2, los dispositivos móviles envían ID de dispositivo como parte del certificado de cliente. El certificado de CA enlazado aquí debe

ser el que se utilice para emitir certificados de cliente para los dispositivos iOS y Android de los usuarios finales. Si hay certificados intermedios, también deben vincularse aquí. Para obtener más información sobre la configuración de Intune, consulte Configuración de una aplicación NetScaler Gateway en el portal de Azure. Para admitir la API de Intune NAC v2, seleccione el certificado de CA requerido y haga clic en **Vincular**.

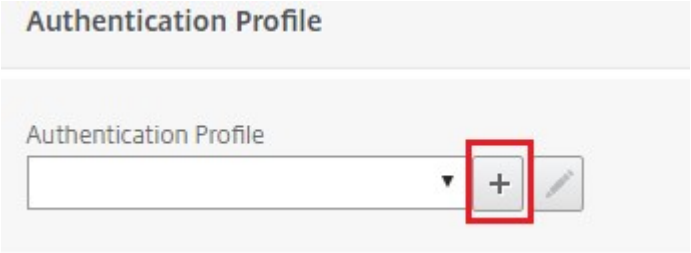


7. Haga clic en **Continuar**.
8. Haga clic en **Continuar**.
9. Haga clic en **Continuar**.
10. Haga clic en el icono del signo más **[+]** junto a **Directivas** y seleccione **Sesión** en la lista **Elegir directiva**, seleccione **Solicitud** en la lista **Elegir tipo** y haga clic en **Continuar**.
11. Haga clic en el icono del signo más **[+]** junto a **Seleccionar directiva**.
12. En la página **Crear directiva de sesión de NetScaler Gateway**, proporcione un nombre para la directiva de sesión.
13. Haga clic en el icono más [+] junto a **Perfil** y, en la página **Crear perfil de sesión de NetScaler Gateway**, proporcione un nombre para el perfil de sesión.
14. En la ficha **Experiencia del cliente**, haga clic en la casilla de verificación situada junto a **Acceso sin cliente** y seleccione **Desactivado** en la lista.
15. Haga clic **en la casilla de verificación situada junto a Tipo de complemento** y seleccione Windows/Mac OS X en la lista.
16. Haga clic en **Configuración avanzada**, seleccione la casilla de verificación situada junto a **Opciones del cliente** y establezca su valor **en**ACTIVADO.

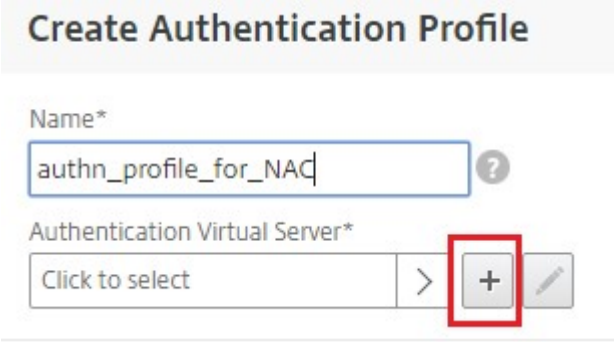
17. En la ficha **Seguridad**, haga clic en la casilla de verificación situada junto a **Acción de autorización predeterminada** y seleccione **Permitir** en la lista.
18. En la ficha **Aplicaciones publicadas**, haga clic en la casilla de verificación situada junto a **Proxy ICA** y seleccione **DESACTIVADO** en la lista.
19. Haga clic en **Crear.**
20. En la página **Crear directiva de sesión de NetScaler Gateway**, en el área **Expresión**, configure la expresión calificadora.
21. Haga clic en **Crear**.
22. Haga clic en **Bind**.
23. Seleccione **Perfil de autenticación** en **Configuración avanzada**.



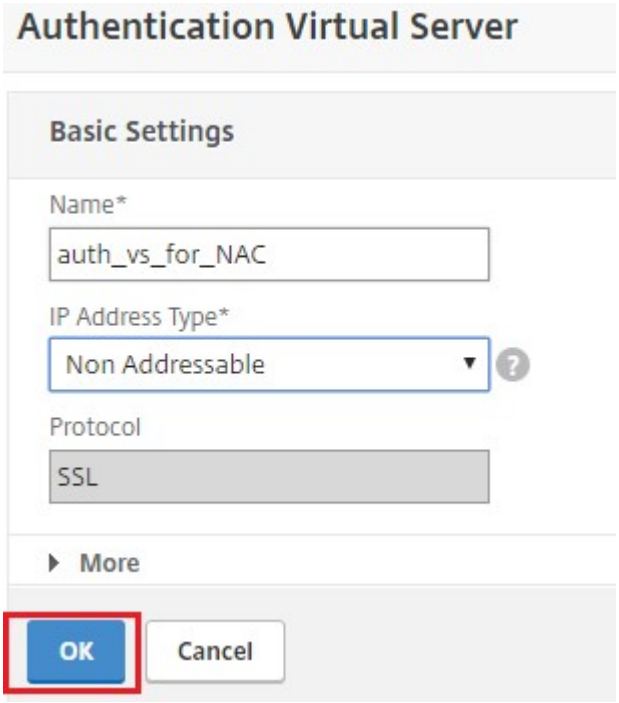
24. Haga clic en el icono más **[+]** y proporcione un nombre para el perfil de autenticación.



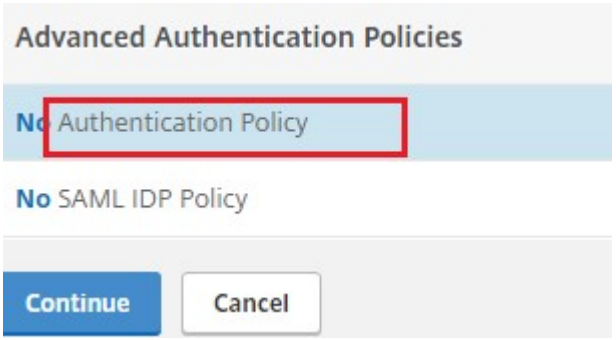
25. Haga clic en el icono más **[+]** para crear un servidor virtual de autenticación.



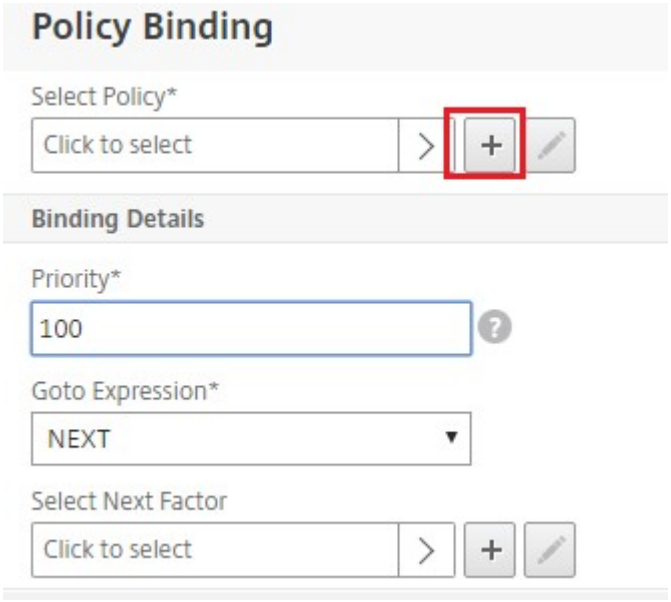
26. Especifique el nombre y el tipo de dirección IP del servidor virtual de autenticación en el área **Configuración básica** y haga clic en **Aceptar**.El tipo de dirección IP también puede **ser No direccionable**.



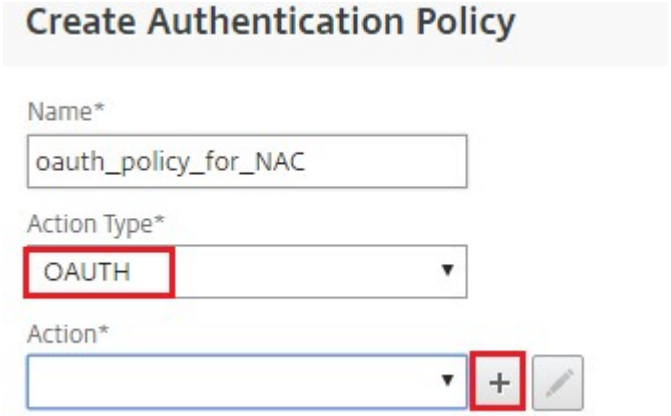
27. Haga clic en **Directiva de autenticación**.



28. En la vista Vinculación de directivas, haga clic en el icono más **[+]** para crear una directiva de autenticación.



29. Seleccione **OAUTH** como **tipo de acción** y haga clic en el icono más **[+]** para crear una acción de OAuth para NAC.



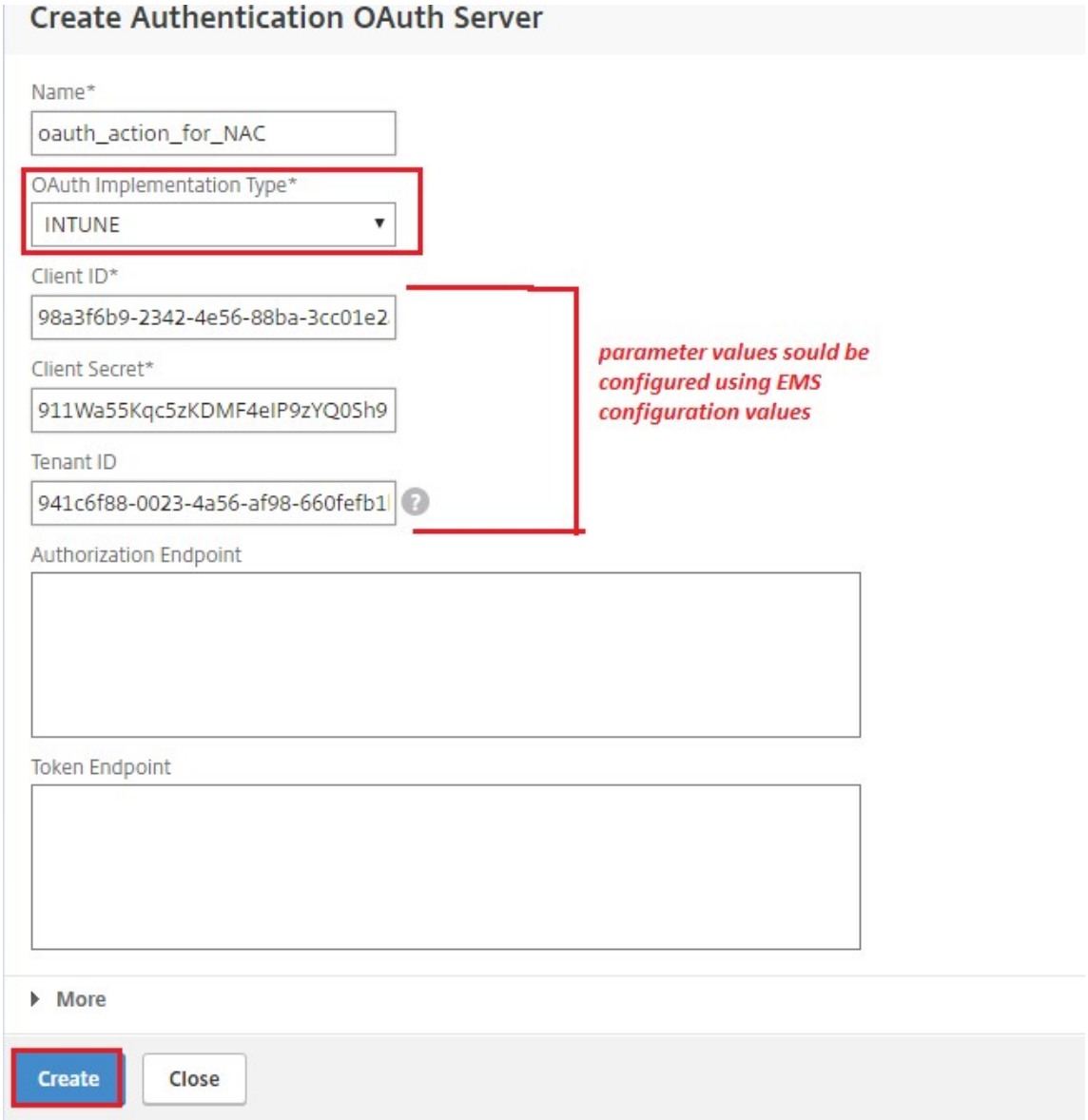
30. Cree una acción de OAuth mediante **ID de cliente**, **secreto de cliente**e **ID de arrendatario**.

> **Nota:**
>
> - El**ID**de **cliente, el secreto** del cliente y el **ID de inquilino** se generan después de configurar la aplicación NetScaler Gateway en el portal de Azure.
> - Anote la información de ID de cliente/ID de aplicación, secreto de cliente/secreto de aplicación e ID de arrendatario de Azure, tal como se requiere para crear una acción de OAuth en NetScaler Gateway más adelante.

Asegúrese de que tiene un servidor de nombres DNS adecuado configurado en el dispositivo para resolverlo y alcanzarlo;
`https://login.microsoftonline.com/`,

-

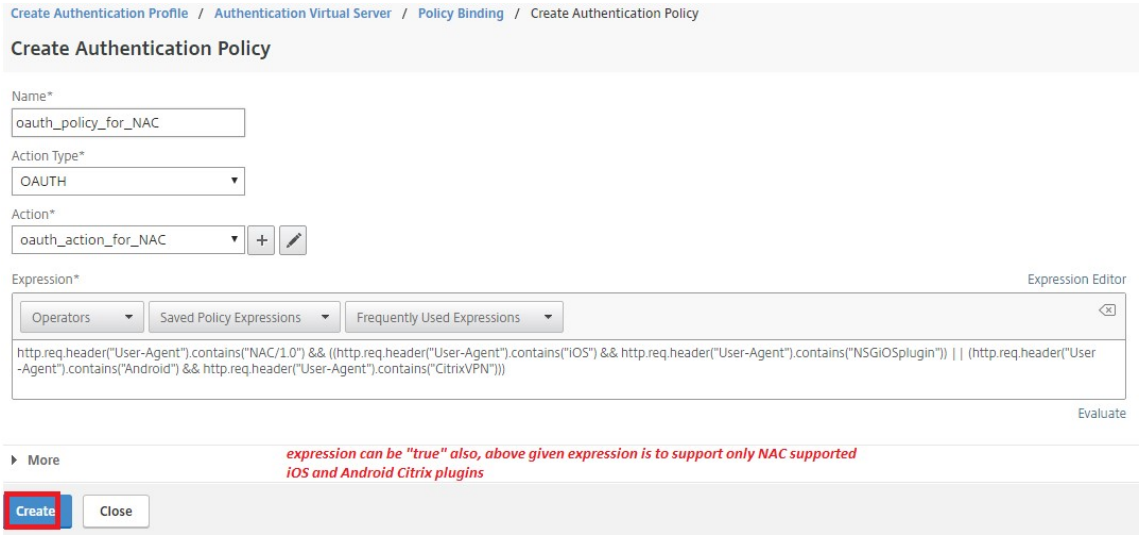
- `https://graph.windows.net/`, - *.manage.microsoft.com.



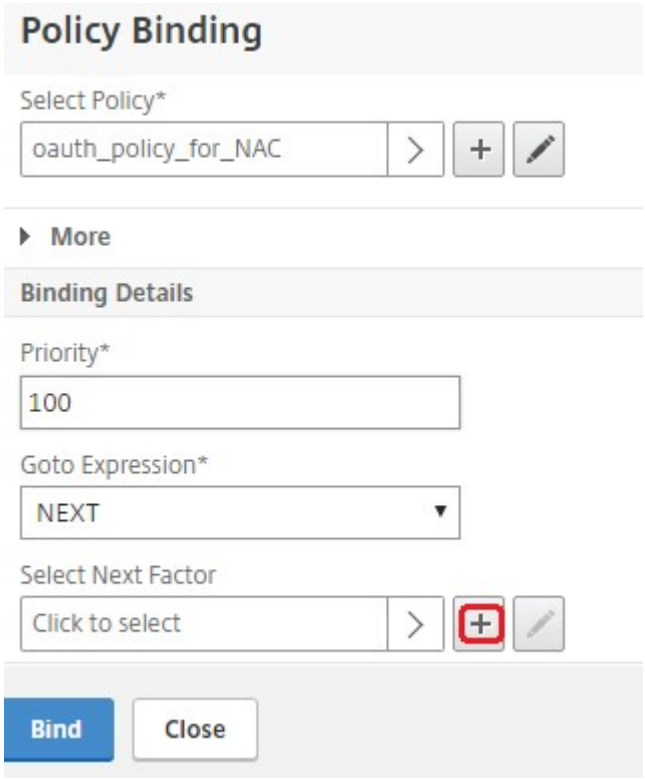
31. Crear directiva de autenticación para **OAuth Action**.

Regla:

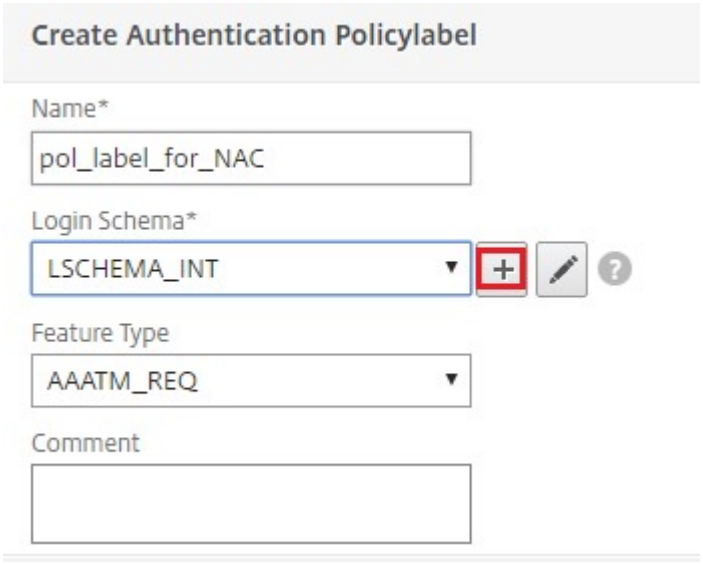
```
http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.
    header("User-Agent").contains("iOS") && http.req.header("User-
    Agent").contains("NSGiOSplugin")) || (http.req.header("User-
    Agent").contains("Android") && http.req.header("User-Agent").
    contains("CitrixVPN")))
<!--NeedCopy-->
```

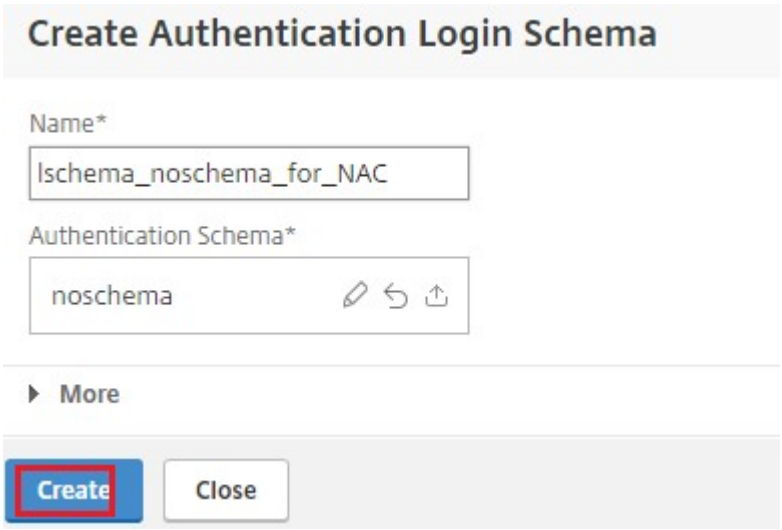
32. Haga clic en el icono más **[+]** para crear una etiqueta de directiva de NextFactor.



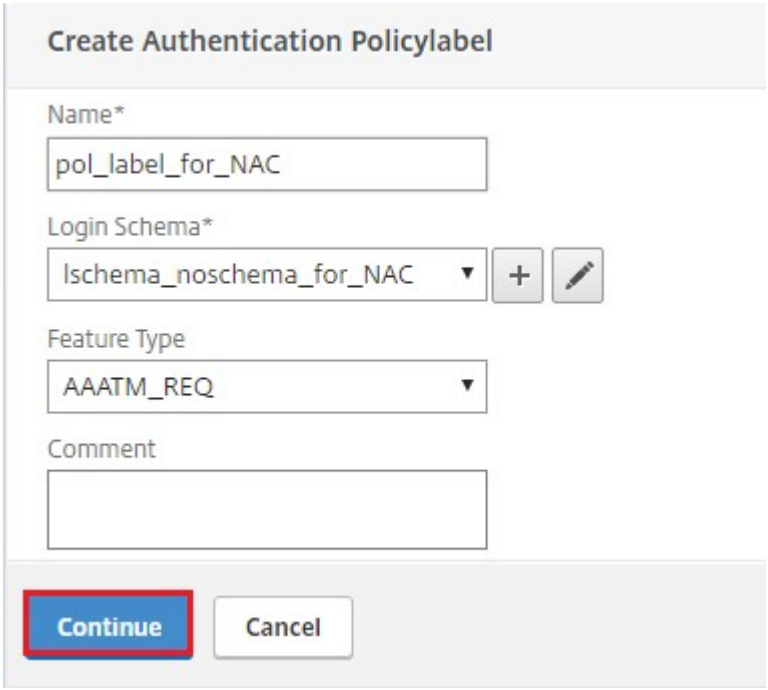
33. Haga clic en el icono más **[+]** para crear un esquema de inicio de sesión.



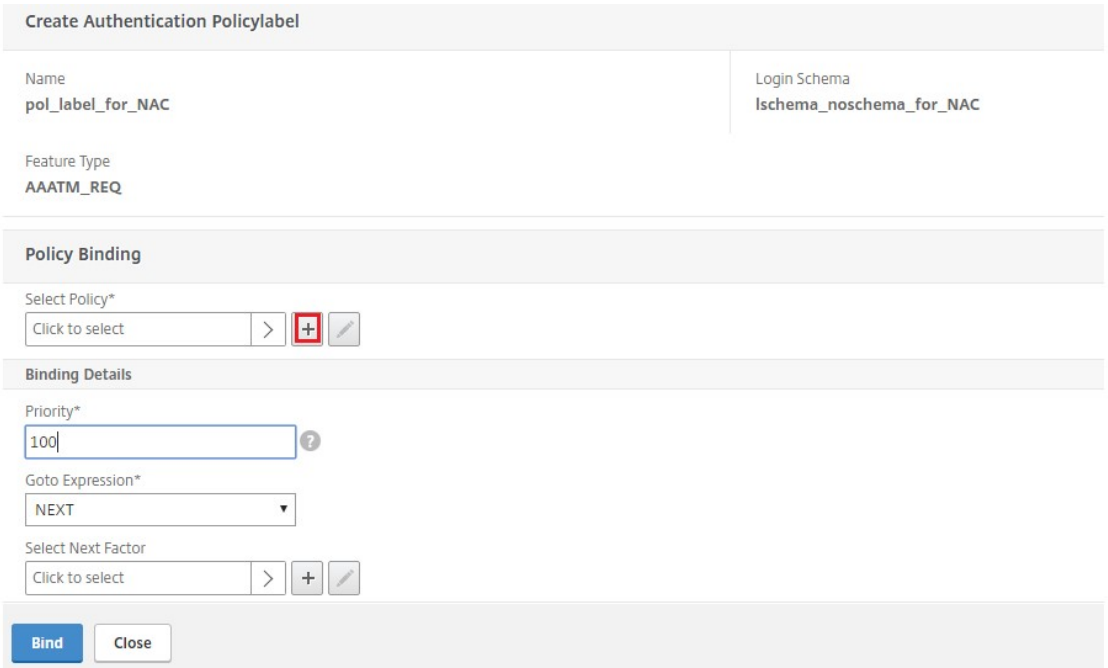
34. Seleccione **noschema** como esquema de autenticación y haga clic en **Crear**.



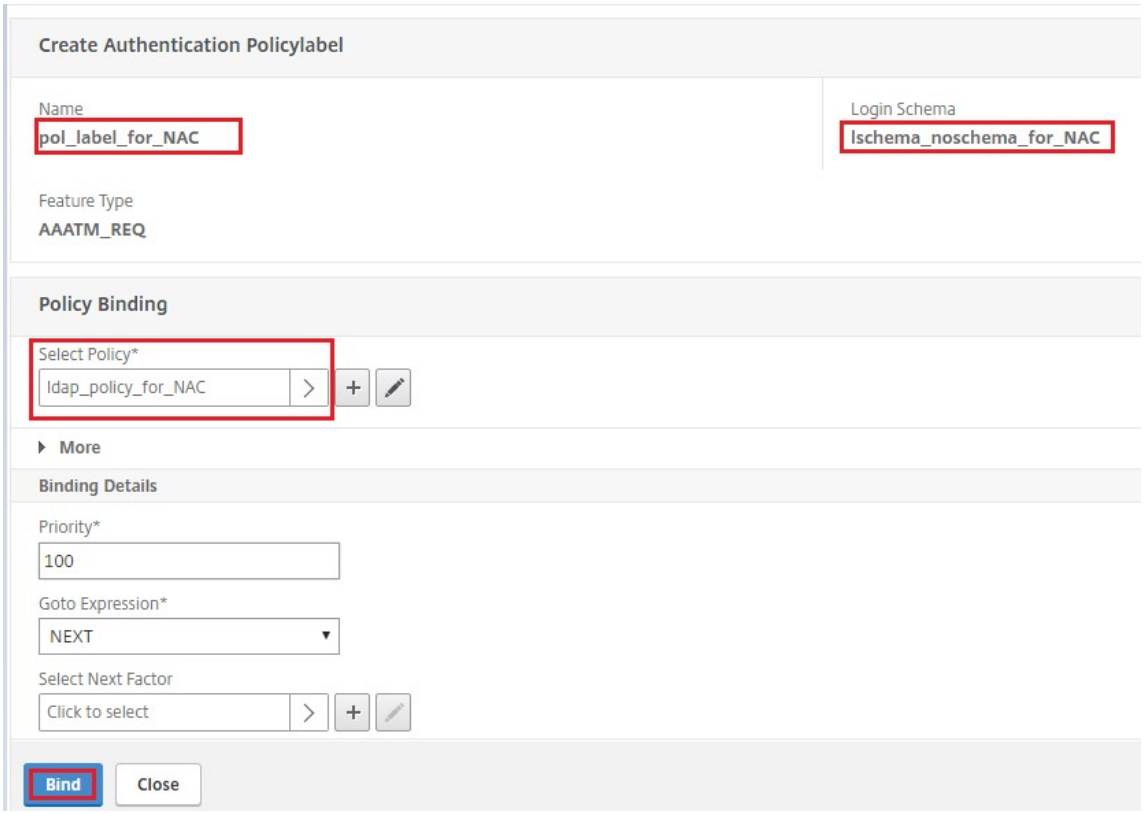
35. Tras seleccionar el esquema de inicio de sesión creado, haga clic en **Continuar**.



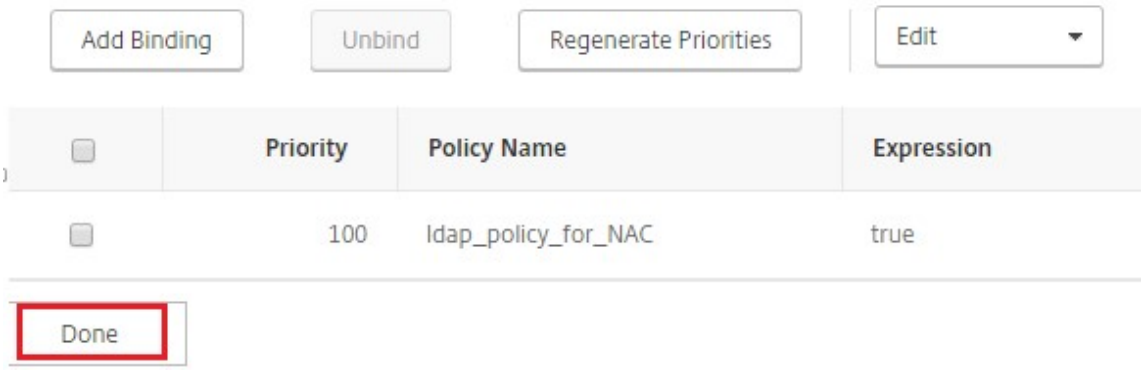
36. En **Seleccionar directiva**, seleccione una directiva de autenticación existente para el inicio de sesión de usuario o haga clic en el icono más **+** para crear una directiva de autenticación.
    Para obtener más información sobre cómo crear una directiva de autenticación, consulte Configuración de directivas de autenticación avanzadas y Configuración de la autenticación LDAP.



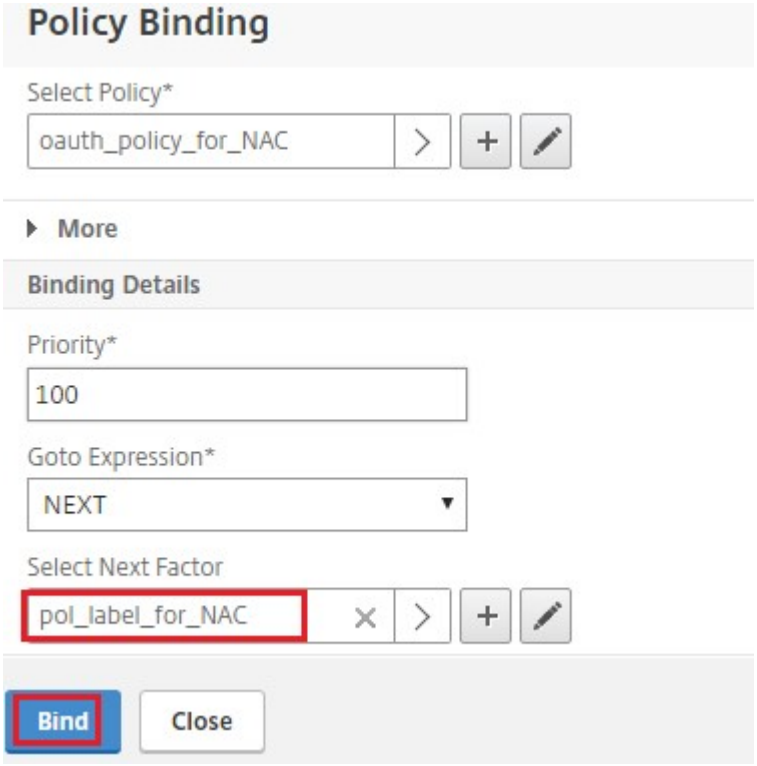
37. Haga clic en **Bind**.



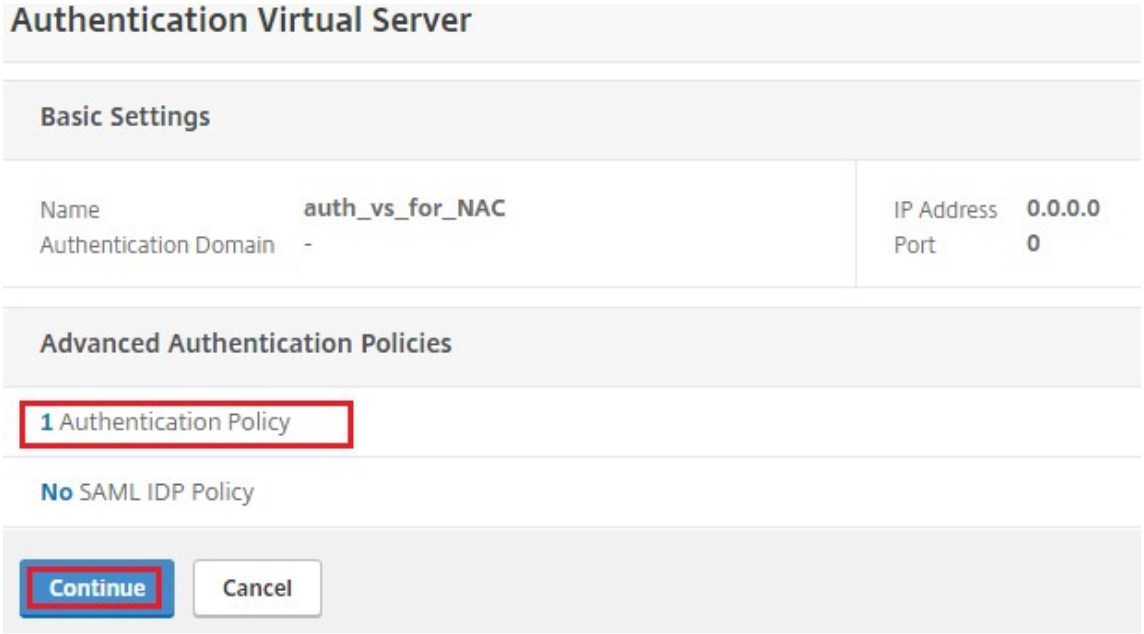
38. Haga clic en **Listo**.



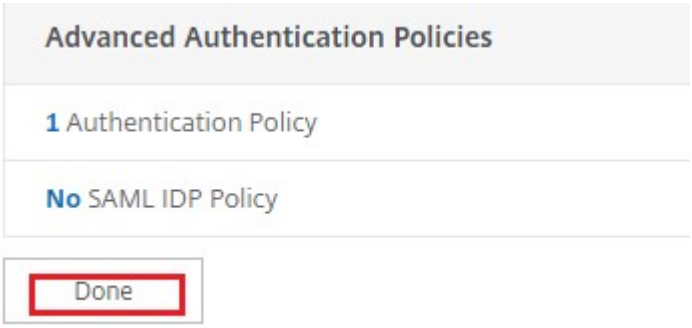
39. Haga clic en **Bind**.



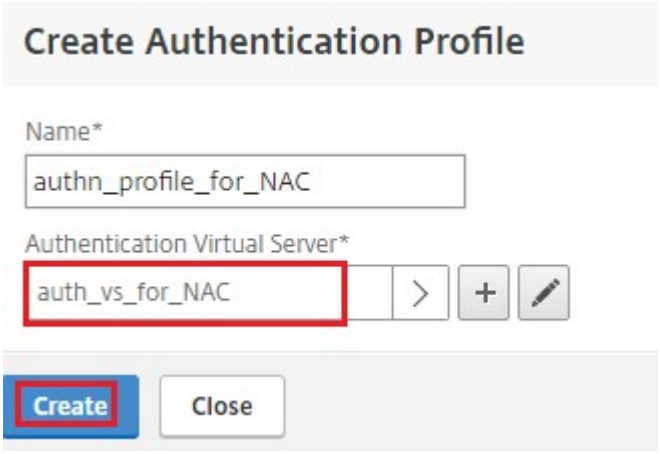
40. Haga clic en **Continuar**.



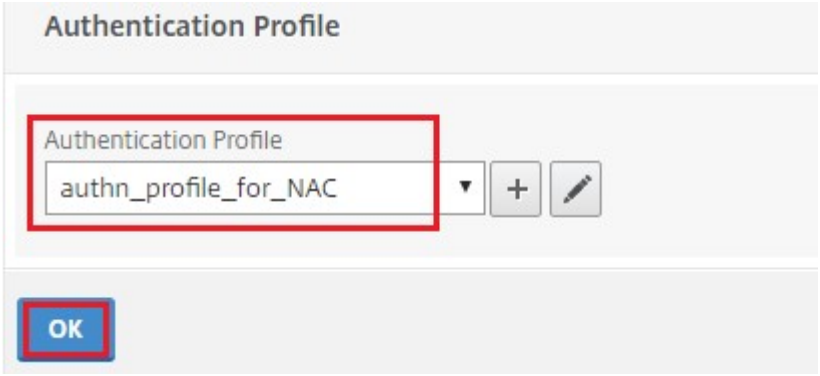
41. Haga clic en **Listo**.



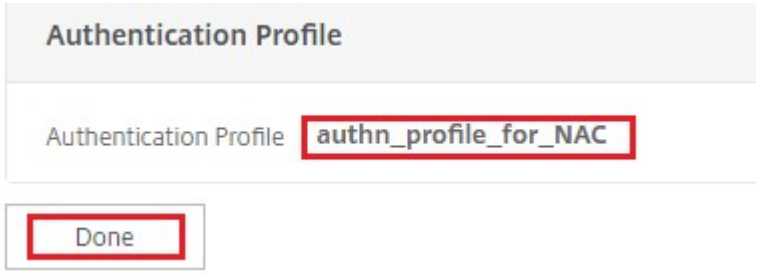
42. Haga clic en **Crear**.



43. Haga clic en **Aceptar**.



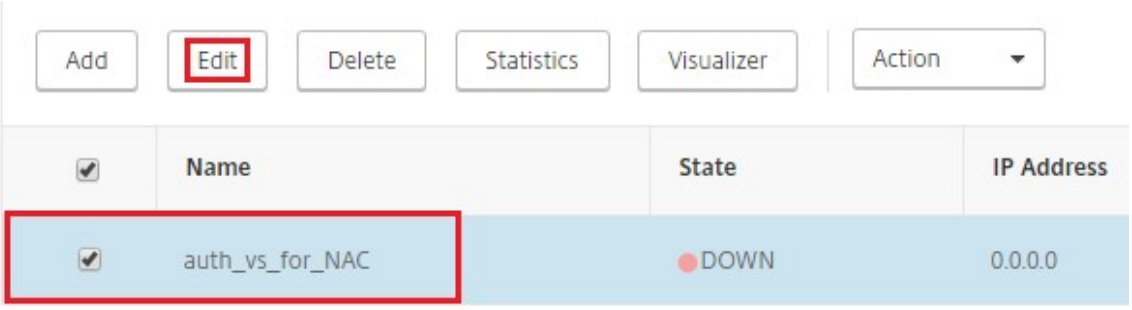
44. Haga clic en **Listo**.



Para enlazar el esquema de inicio de sesión de autenticación al servidor virtual de autenticación para indicar que los complementos VPN deben enviar el ID de dispositivo como parte de la solicitud /cgi/login

1. Vaya a **Seguridad** > **AAA - Tráfico de aplicaciones** > **Servidores virtuales**.

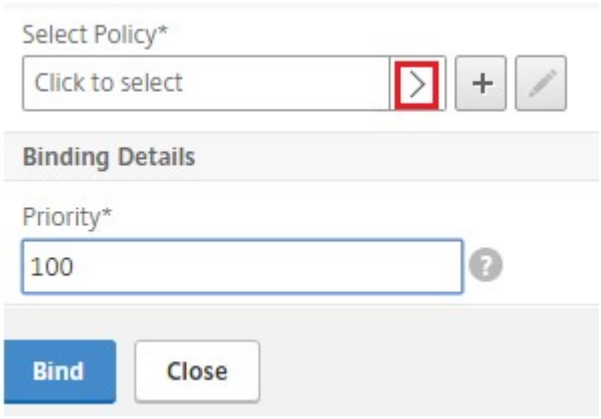
2. Seleccione el servidor virtual seleccionado previamente y haga clic en **Modificar**.



3. Haga clic en **Esquemas de inicio** de sesión en **Configuración avanzada**.

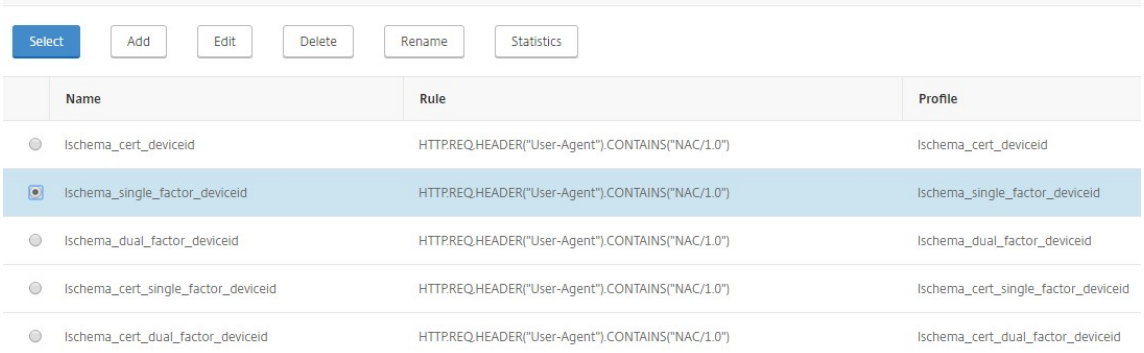
4. Haga clic en **Esquemas de inicio** de sesión para enlazar.

5. Haga clic en **[>]** para seleccionar y vincular las directivas de esquema de inicio de sesión integradas existentes para la verificación del dispositivo NAC.

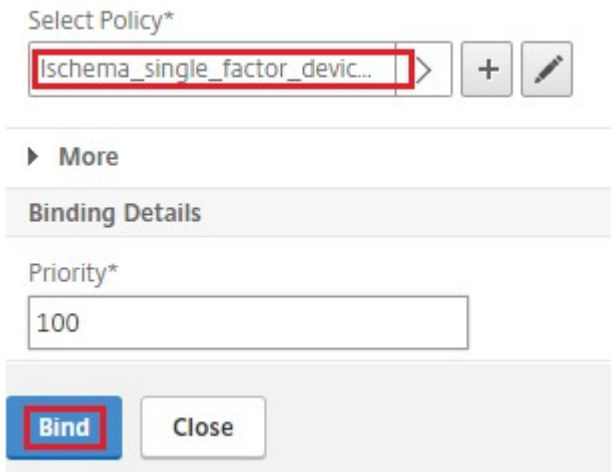


6. Seleccione la directiva de esquema de inicio de sesión necesaria adecuada para su implementación de autenticación y haga clic en **Seleccionar**.

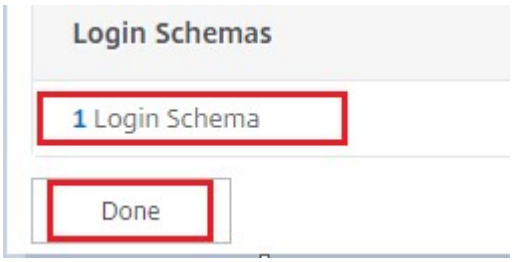
   En la implementación explicada anteriormente, se utiliza la autenticación de factor único (LDAP) junto con una directiva NAC OAuth Action. Por lo tanto, se selecciona **lschema_single_factor_deviceid**.



7. Haga clic en **Bind**.



8. Haga clic en **Listo**.



Compatibilidad con la API Intune NAC v2

Como parte de la compatibilidad con la API de Intune NAC v2, debe vincular un archivo de entidad de certificación (certificado de CA) para garantizar que el dispositivo NetScaler obtenga un certificado válido de los dispositivos móviles. En Intune NAC v2, los dispositivos móviles envían ID de dispositivo como parte del certificado de CA. El certificado de CA enlazado aquí debe ser el que se utilice para emitir certificados de cliente para los dispositivos iOS y Android de los usuarios finales. Si hay certificados intermedios, también deben vincularse aquí.

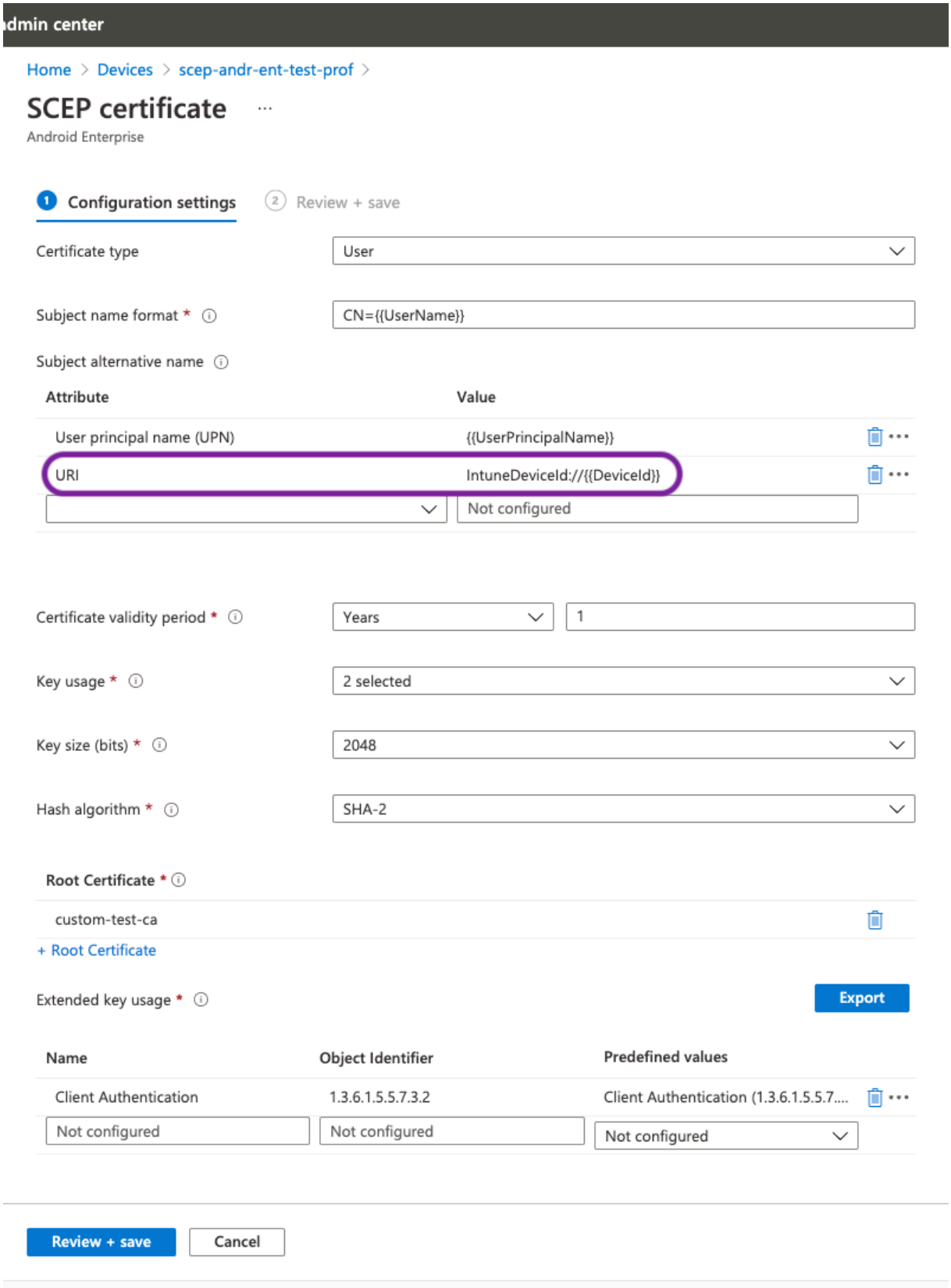
Puede usar el siguiente comando de ejemplo para vincular su certificado de CA.

```
1 bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -
     ocspCheck Optional
2 <!--NeedCopy-->
```

Importante:

- La compatibilidad con la API de Intune NAC v2 está disponible en las versiones de NetScaler Gateway 13.1 compilación 12.50 o posterior y 13.0 compilación 84.11 o posterior.
- Debe habilitar la autenticación basada en certificados de cliente estableciendo `clientAuth` en HABILITADO y `clientCert` en OPCIONAL en los servidores virtuales de autenticación y VPN. El parámetro `clientCert` se establece en OPCIONAL para que otros puntos finales que no necesiten la comprobación de NAC de Intune puedan autenticarse a través del mismo servidor virtual sin proporcionar el certificado de cliente. Los dispositivos Android e iOS deben proporcionar el certificado de cliente. De lo contrario, la comprobación NAC de Intune falla
- Debe asegurarse de que los certificados de cliente aprovisionados a través de Intune en el dispositivo móvil deben tener un identificador de dispositivo de Intune en el campo SAN de tipo URI como se indica en el documento Nuevo servicio de Microsoft Intune para control de acceso a la red. Para obtener información detallada, consulte https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696.

> El formato del campo de valor de URI debe ser el mismo que se indica en esta ilustración. Además, la aplicación Citrix SSO debe usar el mismo certificado para autenticarse con la puerta de enlace.



Solución de problemas

Problemas generales

Problema	La resolución
El mensaje “Agregar directiva requerida”aparece cuando abres una aplicación	Agregar directivas en la API de Microsoft Graph
Hay conflictos de directivas	Solo se permite una única directiva por aplicación
Su aplicación no se puede conectar a los recursos internos	Asegúrese de que los puertos de firewall correctos estén abiertos, que se haya utilizado el ID de arrendatario correcto, etc.

Problemas de NetScaler Gateway

Problema	La resolución
Los permisos necesarios para configurar la aplicación de puerta de enlace en Azure no están disponibles.	Compruebe si dispone de una licencia adecuada de Intune. Pruebe a utilizar el portal manage.windowsazure.com para ver si se puede agregar el permiso. Contacte con la asistencia de Microsoft si el problema persiste.
NetScaler Gateway no puede contactar con `login.microsoftonline.comandgraph.windows.net`.	Desde NS Shell, comprueba si puede acceder al siguiente sitio web de Microsoft: cURL -v -k https://login.microsoftonline.com. A continuación, compruebe si el DNS está configurado en NetScaler Gateway. Compruebe también que la configuración del firewall sea correcta (en caso de que las solicitudes DNS estén protegidas por firewall).
Aparece un error en ns.log después de configurar OAuthAction.	Compruebe si las licencias de Intune están habilitadas y si la aplicación Azure Gateway tiene establecidos los permisos adecuados.
`Sh OAuthAction` no muestra el estado de OAuth como completo.	Consulte la configuración de DNS y los permisos configurados en la aplicación de Azure Gateway.

Problema	La resolución
El dispositivo Android o iOS no muestra la solicitud de autenticación dual.	Compruebe si el ID de dispositivo de factor dual logonSchema está vinculado al servidor virtual de autenticación.

Estado y condición de error de OAuth de NetScaler Gateway

Estado	Condición de error
AADFORGRAPH	Secreto no válido, URL no resuelta, tiempo de espera de la conexión agotado
MDMINFO	*manage.microsoft.comestá caído o es inalcanzable
GRAPH	El punto final del gráfico no está accesible
CERTFETCH	No se puede hablar con el token del dispositivo de punto final https://login.microsoftonline.com debido a un error de DNS. Para validar esta configuración, vaya a la solicitud de Shell y escriba cURL https://login.microsoftonline.com. Este comando debe validarse.

Nota: Cuando el estado de OAuth es correcto, el estado se muestra como COMPLETE.

Comprobación de configuración de Intune

Asegúrese de seleccionar la casilla **Acepto** en **Configuración básica de VPN para iOS para Citrix SSO > Habilitar el control de acceso a la red (NAC)**. De lo contrario, la comprobación de NAC no funciona.

Configuración de una aplicación NetScaler Gateway en el portal de Azure

March 27, 2024

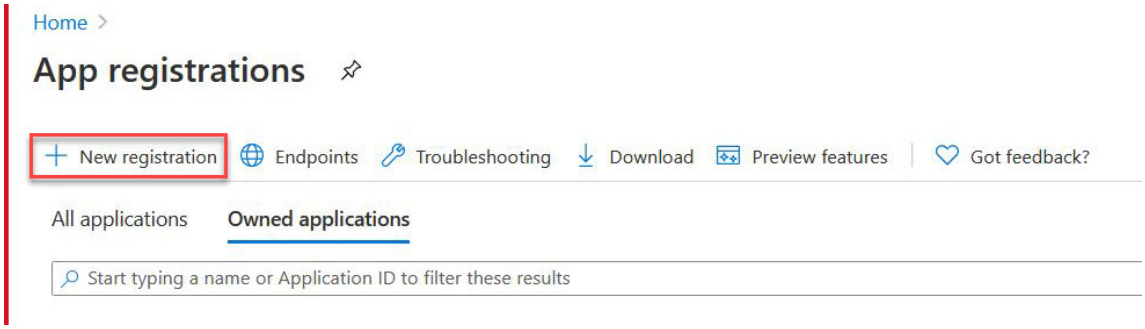
En la siguiente sección se enumeran los pasos para configurar una aplicación NetScaler Gateway en el portal de Azure.

Requisitos previos

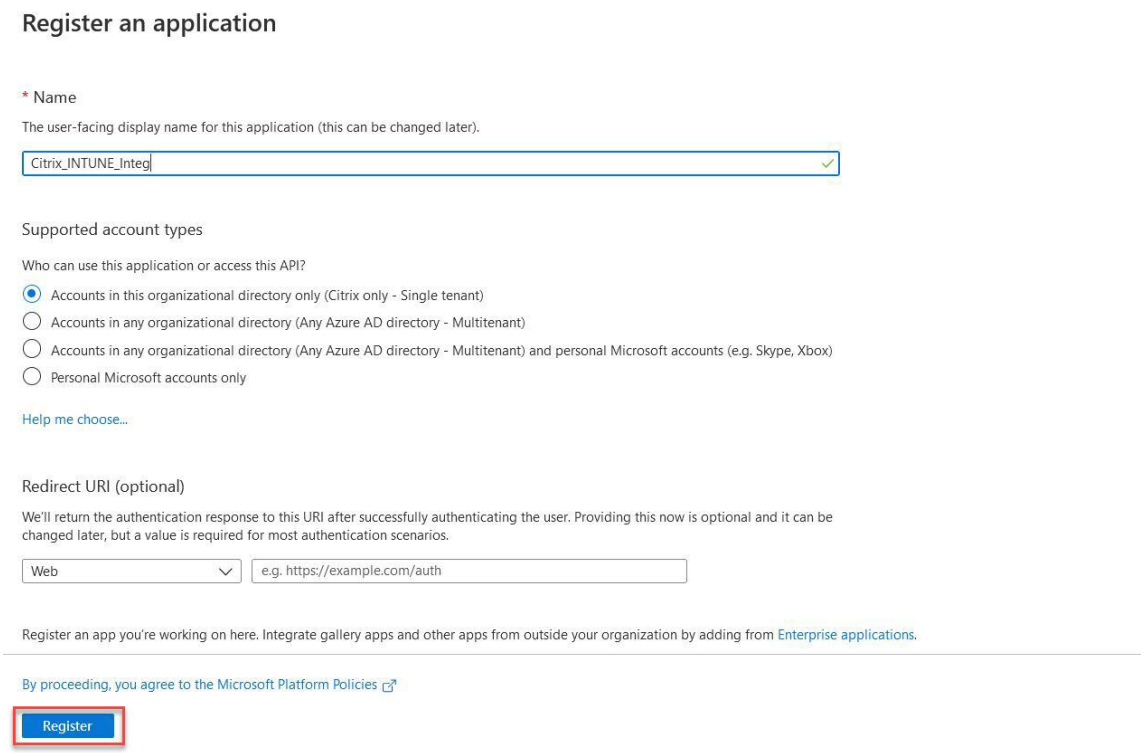
- Credenciales de administrador global de Azure
- La licencia de Intune está habilitada
- Para la integración con Intune, debe crear una aplicación NetScaler Gateway en el portal de Azure.
- Una vez creada la aplicación NetScaler Gateway, configure la directiva OAuth en NetScaler Gateway mediante la siguiente información específica de la aplicación:
  - ID de cliente/ ID de aplicación
  - Secreto de cliente/clave de aplicación
  - Identificador Azure arrendatario
- NetScaler Gateway utiliza el identificador de cliente de la aplicación y el secreto del cliente para comunicarse con Azure y comprobar el cumplimiento de NAC.

Para crear una aplicación NetScaler Gateway en Azure

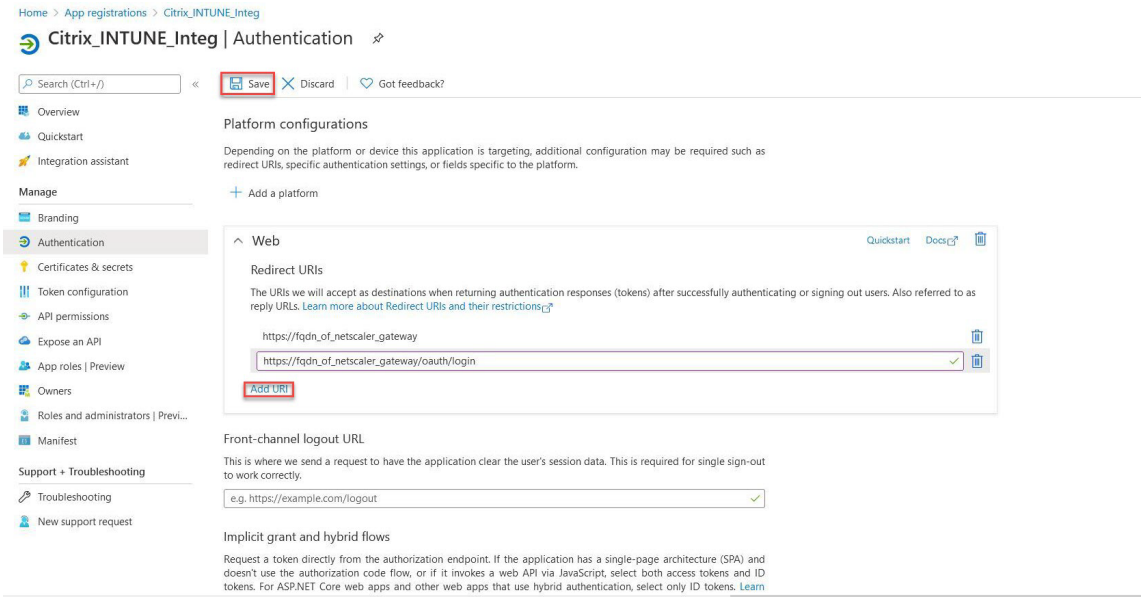
1. Inicia sesión en portal.azure.com
2. Haga clic en **Azure Active Directory**.
3. Haga clic en **Registros de aplicaciones** y haga clic en **Nuevo registro**.



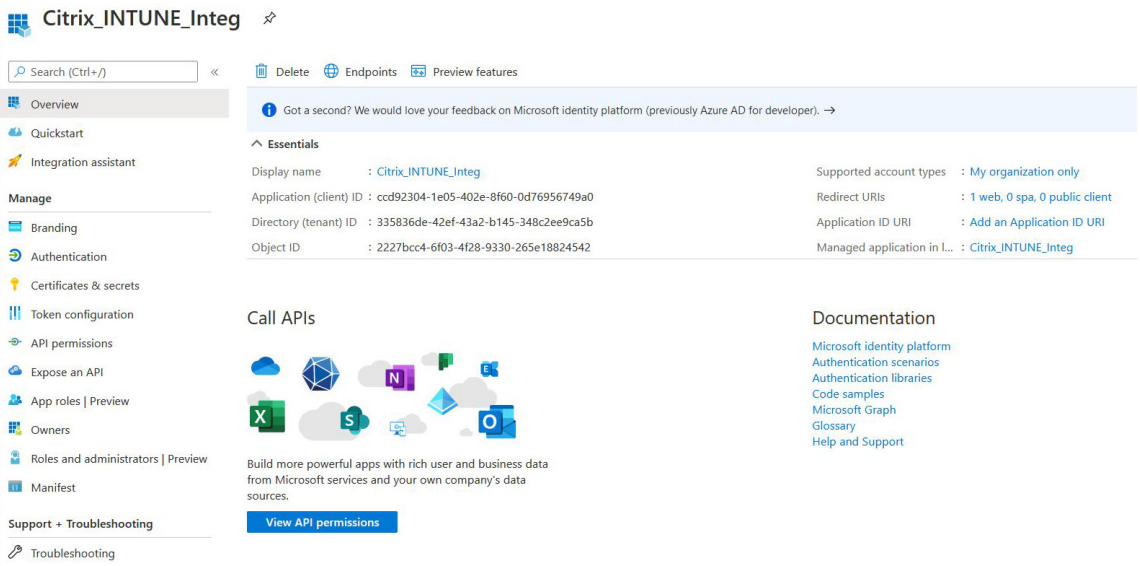
4. En la página **Registrar una aplicación**, introduzca el nombre de una aplicación y haga clic en **Registrar**.



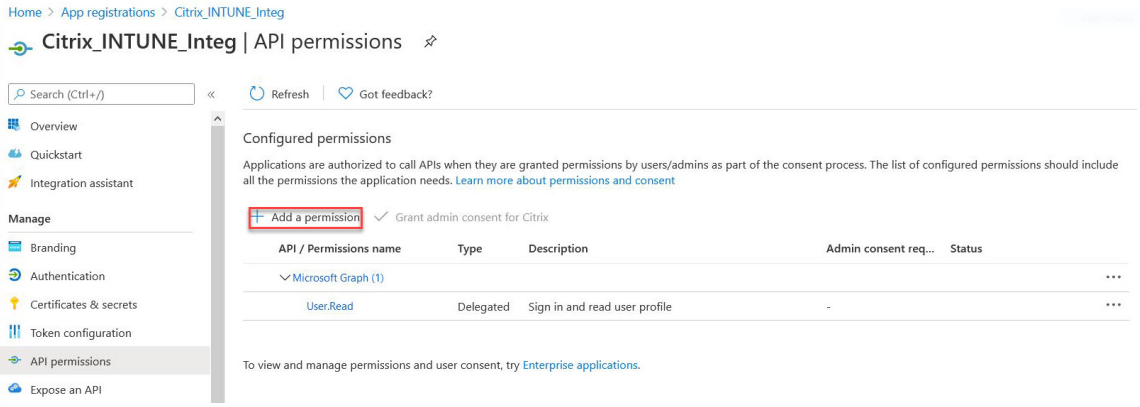
5. Vaya a **Autenticación**, haga clic en **Agregar URI**, escriba FQDN para NetScaler Gateway y haga clic en **Guardar**.



6. Acceda a la página **Visión General** para obtener el ID de cliente, el ID de arrendatario y el ID de objeto.



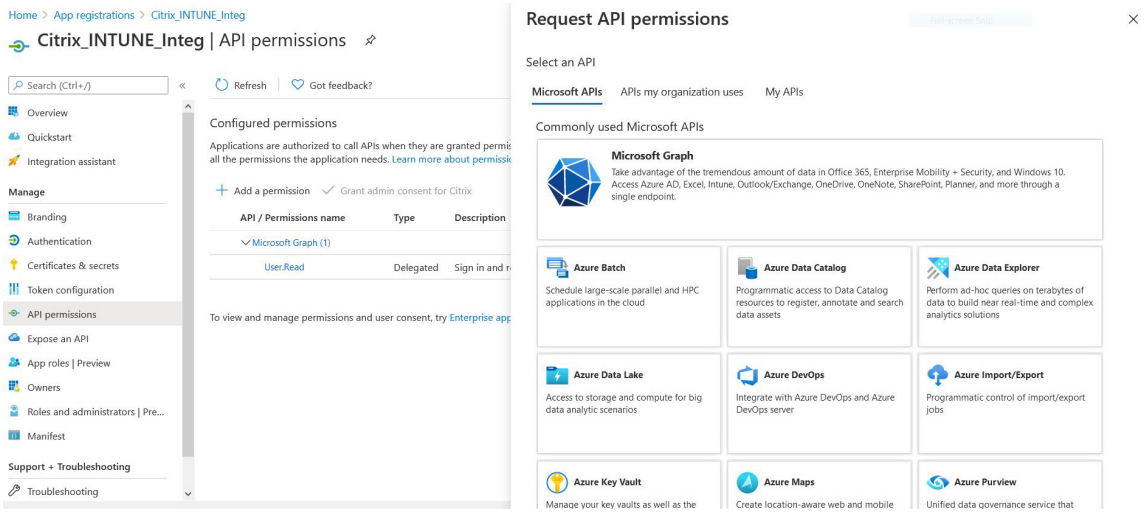
7. Navega hasta **Permisos de API** y haga clic en **Agregar un permiso**.



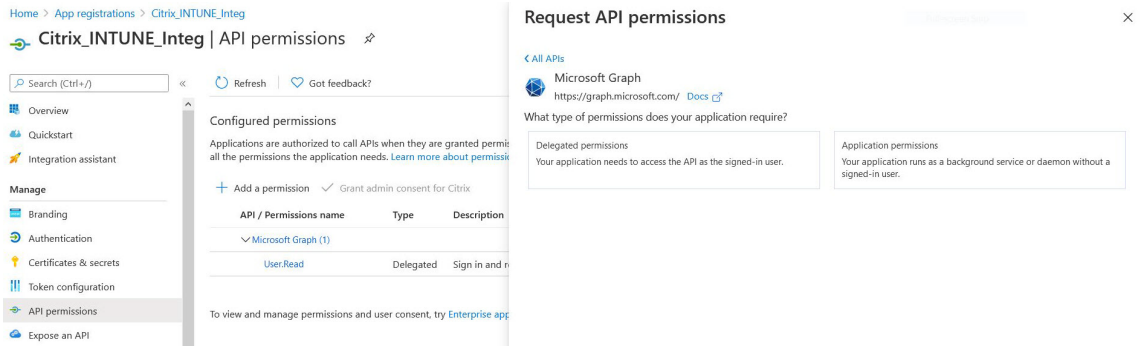
> **Nota:**
>
> Todas las aplicaciones de Azure AD que llaman a los dispositivos de punto final de servicio `https://login.microsoftonline.com`, `https://graph.microsoft.com` o `https://graph.windows.net` requieren que se asigne el permiso de la API para que la puerta de enlace pueda llamar a la API de NAC. Los permisos API disponibles son:
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> El permiso preferido es **Application.Read.All**.
>
> Para obtener más información, consulte https://techcommunity.microsoft.com/t5/intun

> e-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

8. Haga clic en el mosaico **Microsoft Graph** para configurar los permisos de API para Microsoft Graph.

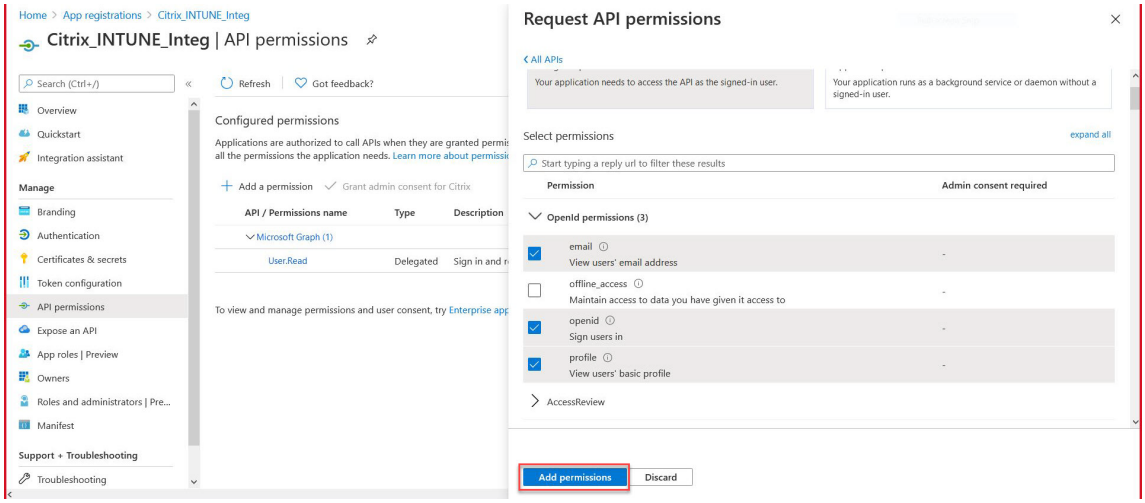


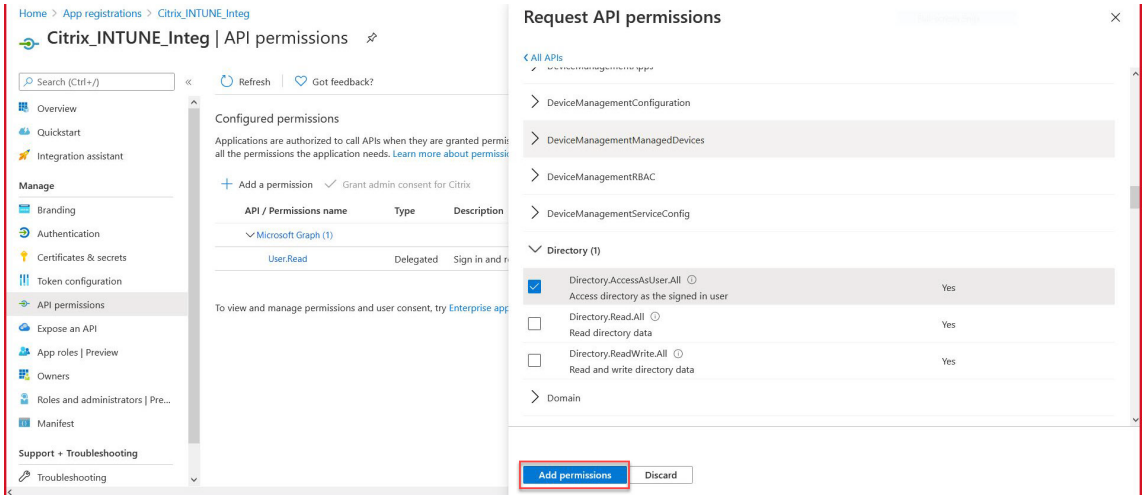
9. Haga clic en el mosaico **Permisos delegados**.

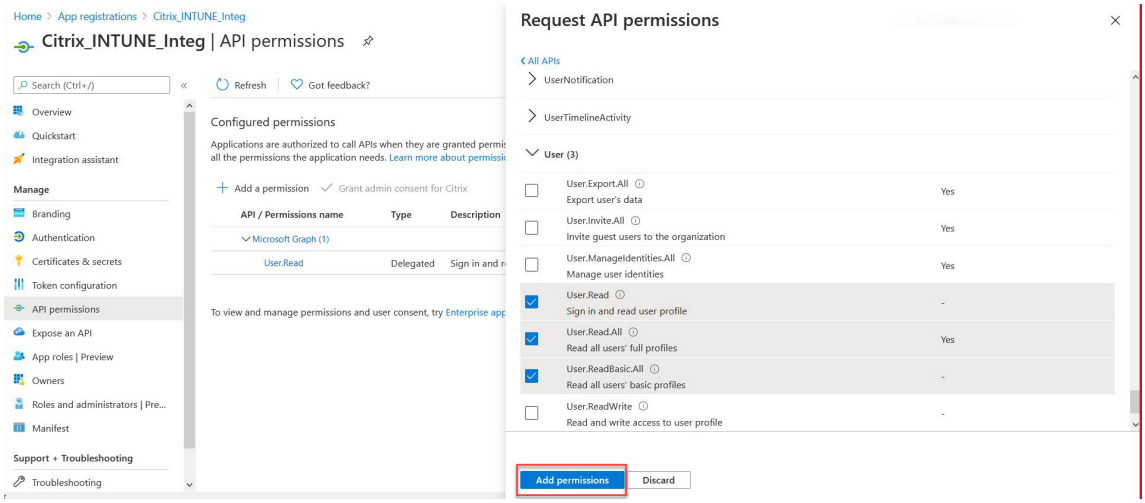


10. Seleccione los siguientes permisos y haga clic en **Agregar permisos**.

    - Correo electrónico
    - `openid`
    - Profile
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All



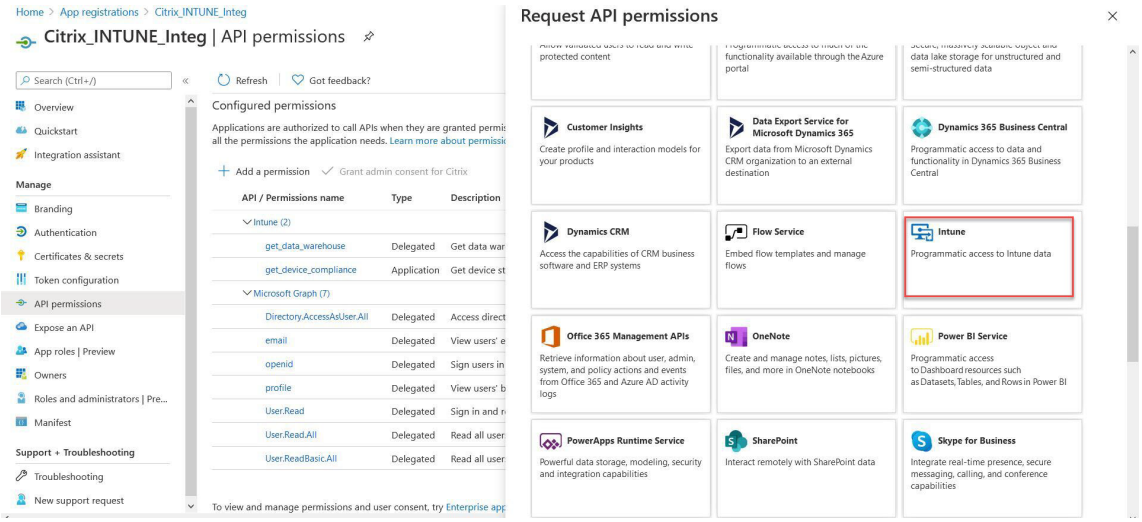




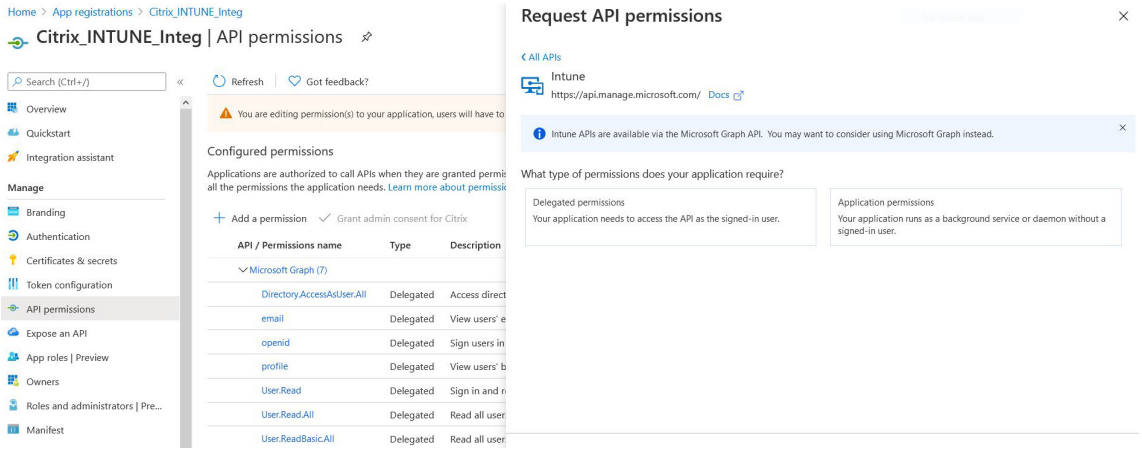
> **Permisos para la comprobación de NAC de Intune:**
>
> Todas las aplicaciones de Azure AD que llaman a los dispositivos de punto final de servicio `https://login.microsoftonline.com`, `https://graph.microsoft.`

> com o `https://graph.windows.net` requieren que se asigne el permiso de la API para que la puerta de enlace pueda llamar a la API de NAC. Los permisos API disponibles son:
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> El permiso preferido es **Application.Read.All**.
>
> Para obtener más información, consulta https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040
>
> **Nota:**
>
> Si un cliente solo usa la comprobación Acción de Intune para NAC, el único permiso necesario es **Application.Read.All** en Microsoft Graph.

11. Haga clic en el icono de **Intune** para configurar los permisos de API para Intune.



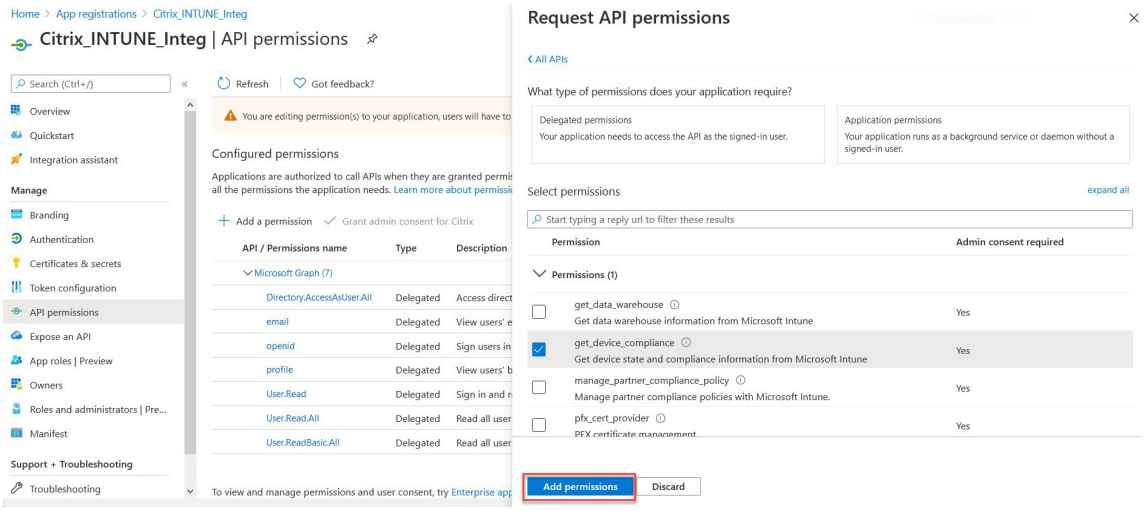
12. Haga clic en el mosaico **Permisos de aplicación** y **Permisos delegados** para agregar permisos para get_device_compliance y get_data_warehouse respectivamente.

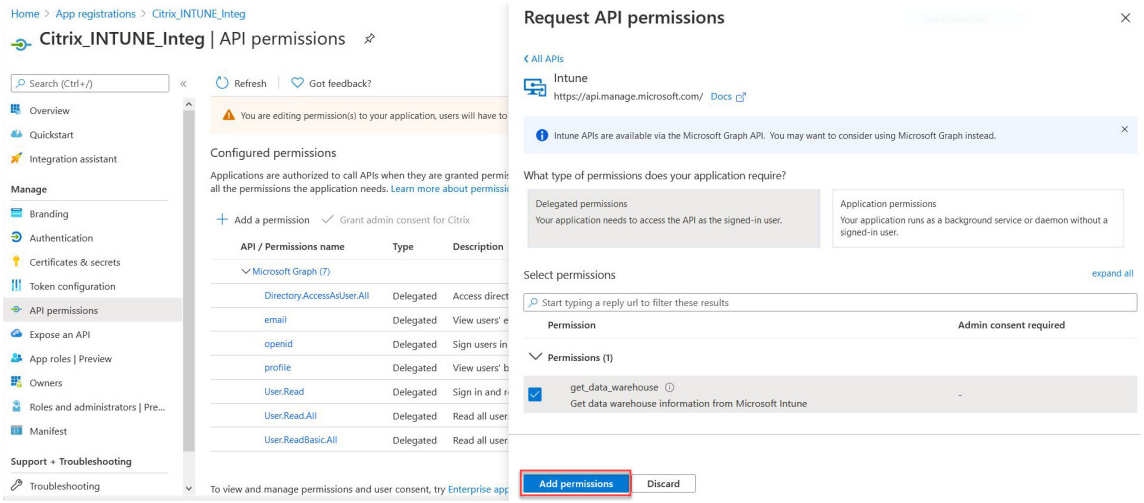


13. Seleccione los permisos siguientes y haga clic en **Agregar permisos**.

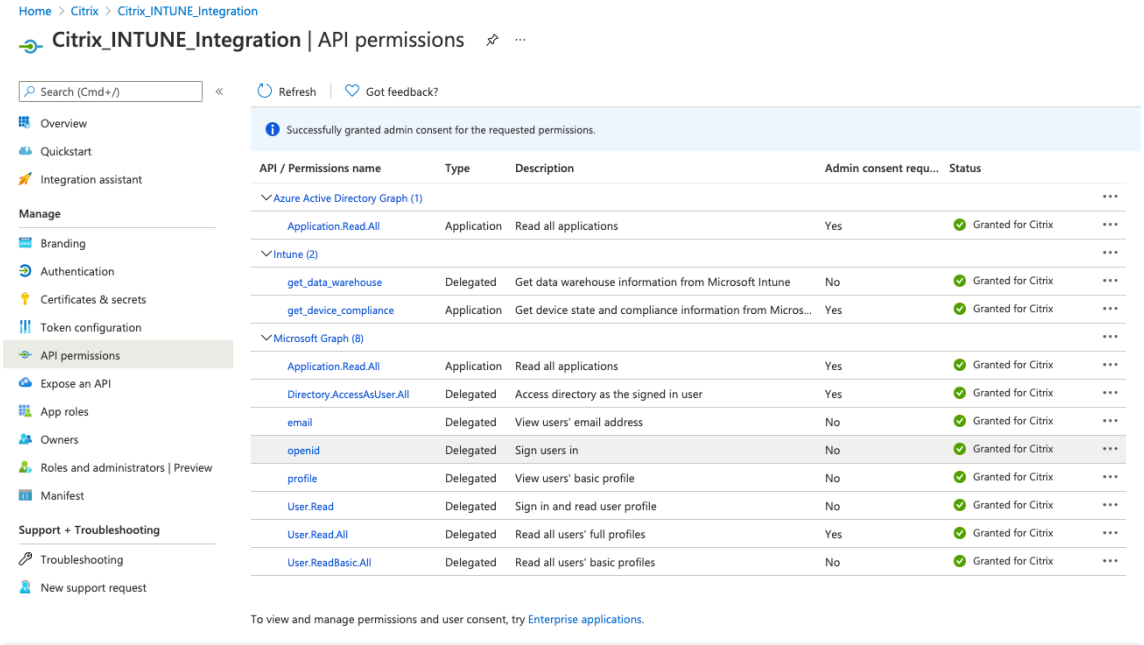
    - get_device_compliance - Permisos de aplicación
    - get_data_warehouse - Permisos delegados

> **Nota:**
>
> Para la comprobación de NAC de Intune, el único permiso necesario es **Get_device_compliance**.

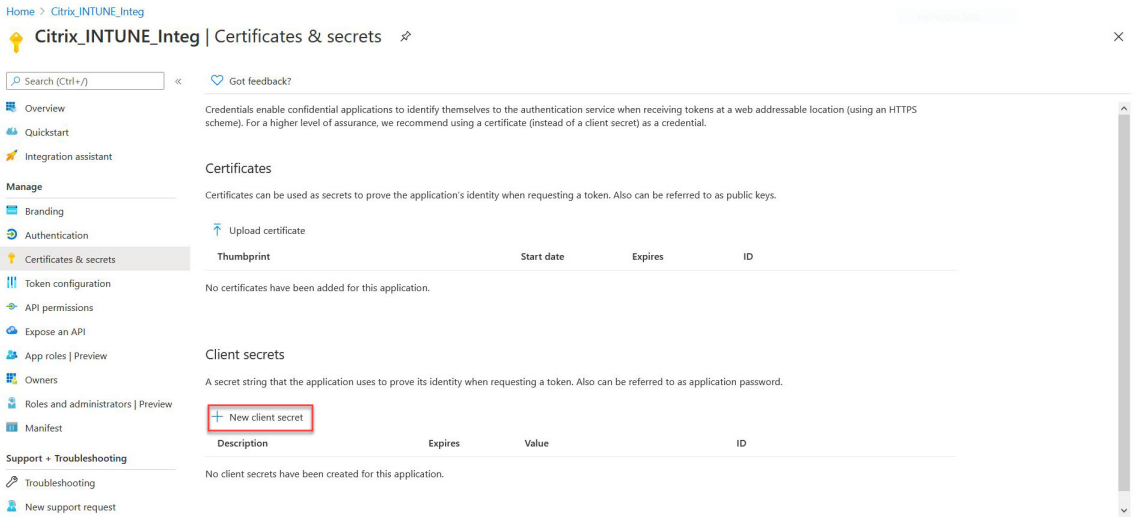




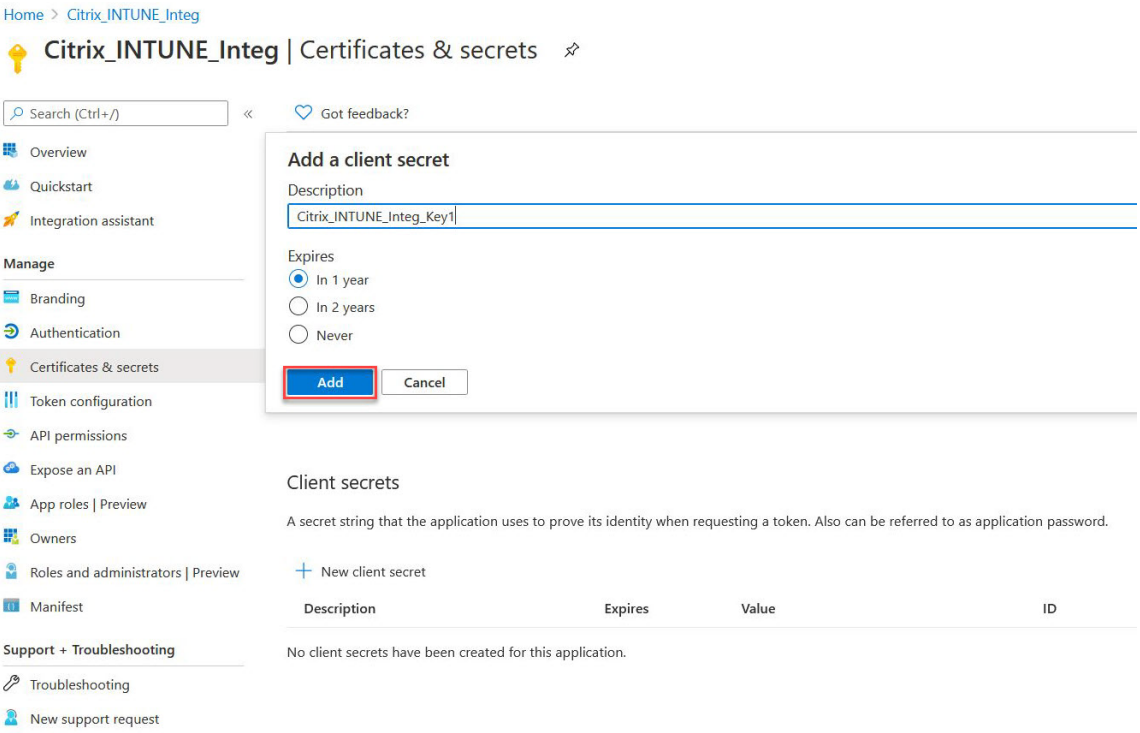
14. En la página siguiente se enumeran los permisos de API configurados.



15. Vaya a **Certificados y secretos** y haga clic en **Nuevo secreto de cliente**.

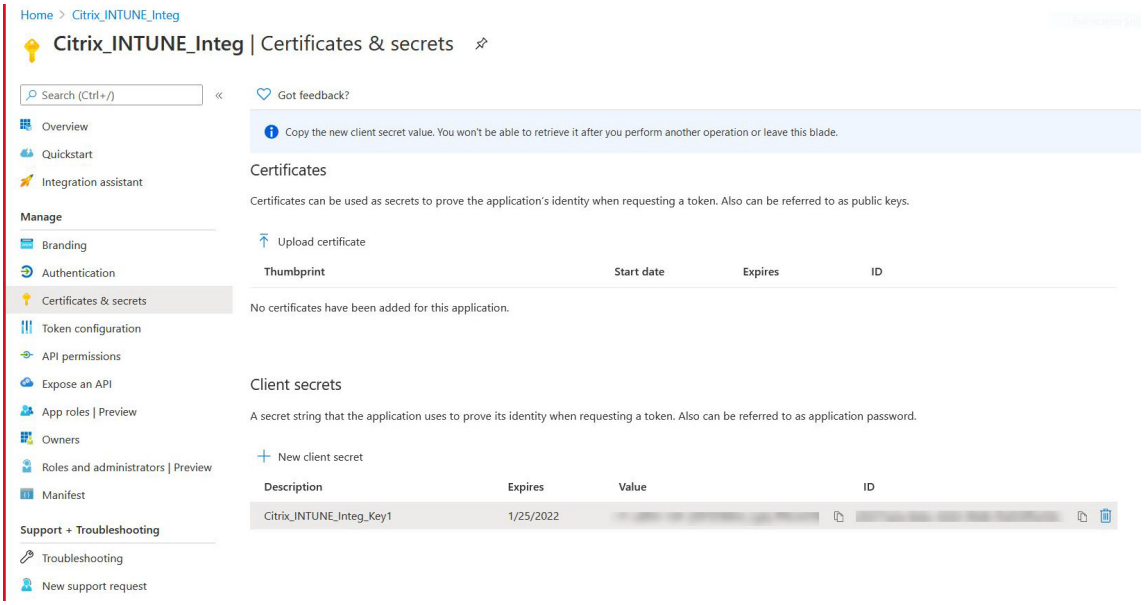


16. En la página **Agregar un secreto de cliente**, introduzca la descripción, seleccione caducidad y haga clic en **Agregar**.



17. En la siguiente pantalla se muestra el secreto del cliente configurado.

> **Nota**
>
> El secreto del cliente solo se muestra una vez cuando se genera. Copie el secreto del cliente mostrado localmente. Utilice el mismo secreto de cliente junto con el ID de cliente asociado a la aplicación recién registrada mientras configura la acción OAuth en el dispositivo NetScaler Gateway para Intune.



La configuración de la aplicación en el portal de Azure se ha completado.

Descripción de la autenticación de tokens ADAL de Azure

January 26, 2024

A continuación se muestra el flujo de eventos en una autenticación de token típica de NetScaler Gateway y Microsoft ADAL:

1. Cuando se inicia una aplicación en iOS o Android, la aplicación se pone en contacto con Azure. Se solicita al usuario que inicie sesión con sus credenciales de usuario. Tras un inicio de sesión satisfactorio, la aplicación recibe un token ADAL.

2. Este token ADAL se presenta en un NetScaler Gateway, que se ha configurado para validar el token ADAL.

3. NetScaler Gateway valida la firma del token ADAL con el certificado correspondiente de Microsoft.

4. Tras una validación satisfactoria, NetScaler Gateway extrae el nombre principal del usuario (UPN) y concede a la aplicación acceso VPN a los recursos internos.

Configurar el servidor virtual de NetScaler Gateway para la autenticación de token ADAL de Microsoft

March 27, 2024

Para configurar un servidor virtual NetScaler Gateway para supervisar la autenticación de tokens ADAL de Microsoft, necesita la siguiente información:

- **CertendPoint**: URL del endpoint que contiene la clave web JSON (JWK) para la verificación del token ADAL.
- **Público**: FQDN del servidor virtual NetScaler al que la aplicación envía el token ADAL.
- **Emisor**: nombre del emisor de AAD. Se rellena de forma predeterminada.
- **tenantID: ID**de arrendatario para el registro de Azure ADAL.
- **ClientID**: ID único que se le da a la aplicación Gateway como parte del registro ADAL.
- **ClientSecret**: clave secreta que se proporciona a la aplicación Gateway como parte del registro de ADAL.
- **resourceURI**: parámetro opcional para capturar el URI del recurso. Si no está configurado, NetScaler utiliza el URI de recursos comerciales de Azure.

Realice los pasos siguientes mediante la interfaz de línea de comandos:

1. Crea una acción de OAuth.

```
add authentication OAuthAction <oauth-action-name> -OAuthType <
    INTUNE>  – clientid <clientID> -clientsecret <client-secret> -
    audience <audience name> -tenantid <tenantID> -issuer <issuer-
    name> -userNameField <upn> -certEndpoint <certEndpoint-name> -
    resourceURI <name of resource URI>
<!--NeedCopy-->
```

2. Cree una directiva de autenticación para asociarla a la acción OAuth recién creada.

```
add authentication Policy <policy-name> -rule <true> -action <
    oauth intune action>
<!--NeedCopy-->
```

3. Enlaza el OAuth recién creado a AuthVS.

```
bind authentication vserver <auth-vserver> -policy <oauth-intune-
    policy> -priority 2 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. Cree un esquema de inicio de sesión.

```
add authentication loginSchema <loginSchemaName> -
    authenticationSchema <authenticationSchema ” location ” >
add authentication loginSchemaPolicy <loginSchemaPolicyName> -rule
     true -action <loginSchemaName>
<!--NeedCopy-->
```

5. Enlazar AuthVS con loginSchema.

```
bind authentication vserver <auth-vs> -policy <oauth-pol> -
    priority 2 -gotoPriorityExpression END
```



```
2 <!--NeedCopy-->
```

6. Agregue un perfil de autenticación y asígnelo a un servidor virtual VPN.

```
1 add authnprofile <nfactor-profile-name> -authnvsName <authvserver>
2 set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name
      >
3 <!--NeedCopy-->
```

Configuración de ejemplo

```
1  add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid
       id 1204 -clientsecret a -audience "[http://hello](http://hello/)" -
       tenantid xxxx -issuer "[https://hello](https://hello/)" -
       userNameField upn -certEndpoint https://login.microsoftonline.com/
       common/discovery/v2.0/keys --resourceURI htpps://api.manage.
       microsoft.com
2
3  add authentication Policy oauth-intune-pol -rule true -action tmp-
       action
4  bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol -
       priority 2 -gotoPriorityExpression END
5
6  add authentication loginSchema oauth-loginschema -authenticationSchema
       "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"
7
8  add authentication loginSchemaPolicy oauth-loginschema-pol -rule true -
       action oauth-loginschema `
9
10 bind authentication vserver auth-vs-for-gw1-intune -policy oauth-
       loginschema-pol -priority 2 -gotoPriorityExpression END
11
12 add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-
       intune
13
14 set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
15 <!--NeedCopy-->
```

Configurar NetScaler Gateway para utilizar micro VPN con Microsoft Endpoint Manager

March 27, 2024

La integración de micro VPN de Citrix con Microsoft Endpoint Management permite que sus aplicaciones accedan a los recursos locales. Para obtener más información, consulte Integración de micro VPN de Citrix con Microsoft Endpoint Manager.

Requisitos del sistema

- Versiones NetScaler Gateway
  - 13.1
  - 13.0
  - 12.1.50.x o posterior
  - 12.0.59.x o posterior

  Puede descargar la versión más reciente de NetScaler Gateway desde la página de descargas de NetScaler Gateway.
- Un escritorio con Windows 7 o posterior (solo para empaquetar aplicaciones Android)
- Microsoft
  - Acceso a Azure AD (con privilegios de administrador de arrendatarios)
  - Arrendatario compatible con Intune
- Reglas de firewall
  - Habilitar una regla de firewall para el tráfico SSL desde una IP de subred de NetScaler Gateway a `*.manage.microsoft.com`, `https://login.microsoftonline.com` y `https://graph.windows.net` (puerto 443)
  - NetScaler Gateway debe poder resolver externamente las URL anteriores.

Requisitos previos

- **Entorno de Intune:** si no tiene un entorno Intune, configura uno. Para obtener instrucciones, consulte la documentación de Microsoft.
- **Aplicación Edge Browser:** El SDK de Micro VPN está integrado en la aplicación Microsoft Edge y en la aplicación Intune Managed Browser para iOS y Android. Para obtener más información acerca de Managed Browser, consulte la página de Managed Browser de Microsoft.
- **Derecho de uso Citrix Endpoint Management**: Asegúrese de tener derechos de uso de Citrix Endpoint Management activo para seguir admitiendo el SDK de micro VPN en exploradores web móviles de Microsoft Edge (iOS y Android). Para obtener más información, contacte con su representante de ventas, cuentas o socios.

Conceder permisos a aplicaciones de Azure Active Directory (AAD)

1. Consentimiento a la aplicación AAD multiarrendatario de Citrix para permitir que NetScaler Gateway se autentique con el dominio AAD. El administrador global de Azure debe visitar la siguiente URL y dar su consentimiento:

https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent.

2. Consentimiento a la aplicación AAD multiarrendatario de Citrix para permitir que las aplicaciones móviles se autentiquen con la micro VPN de NetScaler Gateway. Este enlace solo es necesario si el administrador global de Azure ha cambiado el valor predeterminado para que los usuarios puedan registrar aplicaciones de Sí a No.
   Esta configuración se encuentra en el portal de Azure en **Azure Active Directory > Usuarios > Configuración de usuario**.
   El administrador global de Azure debe visitar la siguiente URL y dar su consentimiento (agregue su ID de
   arrendatario) https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7.

Configurar NetScaler Gateway para micro VPN

Para usar una micro VPN con Intune, debe configurar NetScaler Gateway para que se autentique en Azure AD. Un servidor virtual de NetScaler Gateway que ya exista no funciona para este caso de uso. En primer lugar, configure Azure AD para que se sincronice con Active Directory local. Este paso es necesario para que la autenticación entre Intune y NetScaler Gateway se realice correctamente.

Script de descarga: El archivo.zip incluye un archivo léame con instrucciones para implementar el script. Debe introducir manualmente la información que requieren los scripts y ejecutarlos en NetScaler Gateway para configurar el servicio. Puede descargar el archivo de script desde la página de descargas de NetScaler.

> **Importante:** Una vez completada la configuración de NetScaler Gateway y si ve el estado de OAuth distinto de COMPLETE, consulte la sección Solución de problemas.

Configuración del explorador Microsoft Edge

1. Inicie sesión en https://endpoint.microsoft.com/ y, a continuación, vaya a **Intune > Aplicaciones móviles**.
2. Publique la aplicación Edge como lo hace normalmente y, a continuación, agregue una directiva de configuración de aplicaciones.
3. En **Administrar**, haga clic en **Directivas de configuración de aplicaciones**.
4. Haga clic en **Agregar** y, a continuación, escriba un nombre para la directiva que quiere crear. En **Tipo de inscripción de dispositivos**, selecciona **Aplicaciones administradas**.
5. Haga clic en **Aplicación asociada.**
6. Seleccione las aplicaciones a las que quiere aplicar la directiva (explorador administrado de Microsoft Edge o Intune) y, a continuación, haga clic en **Aceptar**.

7. Haga clic en las **opciones de configuración**.
8. En el campo **Nombre**, introduzca el nombre de una de las directivas enumeradas en la tabla siguiente.
9. En el campo del **valor**, escriba el valor que quiere aplicar a esa directiva. Haga clic fuera del campo para agregar la directiva a la lista. Puede agregar varias directivas.
10. Haga clic en **Aceptar** y, a continuación, en **Agregar**.

La directiva se agrega a la lista de directivas.

Nombre (iOS/Android)	Valor	Descripción
—	—	—
MvpnGatewayAddress	https://external.companyname.com	URL externa de NetScaler Gateway
MvpnNetworkAccess	MvpnNetworkAccessTunneledWebSSOor Unrestricted	MvpnNetworkAccessTunneledWebSS es el valor predeterminado para la tunelización
MvpnExcludeDomains	Lista separada por comas de nombres de dominio que se van a excluir	Opcional. Default=Vacío
TunnelExcludeDomains	Utilice esta propiedad de cliente para supeditar la lista predeterminada de dominios excluidos. Valor predeterminado=app.launchdarkly.com,cis.citrix.com, cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly .com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose. launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm .citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix. com,ssl.google-analytics.com,stream.launchdarkly.com

> **Nota:** SSO web es el nombre de Secure Browse en la configuración. El comportamiento es el mismo.

- **MvpnNetworkAccess**: MvpnNetworkAccessTunneledWebSSO habilita la redirección HTTP/HTTPS a través de NetScaler Gateway, también conocido como SSO Tunneled-Web. La puerta de enlace responde a los desafíos de autenticación HTTP en línea, lo que proporciona una experiencia de inicio de sesión único (SSO). Para utilizar el SSO web, establezca esta directiva en **MvpnNetworkAccessTunneledWebSSO**. Actualmente, no se admite la redirección completa del túnel. Use **Unrestricted** para dejar desactivada la micro VPN tunelización.
- **MvpnExcludeDomains**: Lista separada por comas de nombres de host o dominio que se excluirán de la redirección a través del proxy web inverso de NetScaler Gateway. Los nombres de host o dominio se excluyen aunque la configuración de DNS dividida configurada por NetScaler Gateway podría seleccionar el dominio o el host.

> **Nota:**
>
> - Esta directiva solo se aplica a las conexiones **MvpnNetworkAccessTunneledWebSSO**. Si `MvpnNetworkAccess` **no está restringido**, esta directiva se ignora.
> - Esta directiva solo se aplica al modo SSO web en túnel con NetScaler Gateway configurado para la tunelización dividida inversa.

- **TunnelExcludeDomains**: De forma predeterminada, MDX excluye algunos puntos finales de servicio de los túneles de micro VPN. Los SDK de aplicaciones móviles y las aplicaciones utilizan estos puntos finales de servicio para diversas funciones. Por ejemplo, los puntos finales de servicio incluyen servicios que no requieren enrutamiento a través de redes empresariales, como los servicios de Google Analytics, Citrix Cloud y Active Directory. Utilice esta propiedad de cliente para anular la lista predeterminada de dominios excluidos.

  Para configurar esta directiva de cliente global, en la consola de Microsoft Endpoint Management, vaya a **Configuración > Propiedades del cliente**, agregue la clave personalizada **TUNNEL_EXCLUDE_DOMAINS**y establezca el valor.

  Valor: Para reemplazar la lista predeterminada por los dominios que desea excluir de la tunelización, escriba una lista de sufijos de dominio separados por comas. Para incluir a todos los dominios en el túnel, escriba none. El valor predeterminado es:

  ```
  app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis
  -test.citrix.com,clientstream.launchdarkly.com,crashlytics.com
  ,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,
  hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf
  .citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.
  google-analytics.com,stream.launchdarkly.com
  ```

Solución de problemas

Problemas generales

Problema	La resolución
El mensaje “Agregar directiva requerida”aparece cuando abres una aplicación	Agregar directivas en la API de Microsoft Graph
Hay conflictos de directivas	Solo se permite una única directiva por aplicación

Problema	La resolución
El mensaje “No se pudo empaquetar la aplicación”aparece al empaquetar una aplicación. Para ver el mensaje completo, consulte la tabla siguiente	La aplicación está integrada con el SDK de Intune. No es necesario empaquetar la aplicación con Intune
Su aplicación no se puede conectar a los recursos internos	Asegúrese de que los puertos de firewall correctos estén abiertos, corrija el ID de arrendatario, etc.

Error al empaquetar el mensaje de error de aplicación:

Error al empaquetar la aplicación. com.microsoft.intune.mam.apppackager.utils.AppPackagerException: Esta aplicación ya tiene integrado el
SDK de MAM.
com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)
La aplicación no puede estar empaquetada.

Problemas de NetScaler Gateway

Problema	La resolución
Los permisos necesarios para configurar la aplicación de puerta de enlace en Azure no están disponibles.	Compruebe si dispone de una licencia adecuada de Intune. Pruebe a utilizar el portal manage.windowsazure.com para ver si se puede agregar el permiso. Contacte con la asistencia de Microsoft si el problema persiste.
NetScaler Gateway no puede contactar con `login.microsoftonline.com and graph.windows.net`.	Desde NS Shell, comprueba si puede acceder al siguiente sitio web de Microsoft: cURL -v -k https://login.microsoftonline.com. A continuación, compruebe si el DNS está configurado en NetScaler Gateway. Compruebe también que la configuración del firewall sea correcta (en caso de que las solicitudes DNS estén protegidas por firewall).

Problema	La resolución
Aparece un error en ns.log después de configurar OAuthAction.	Compruebe si las licencias de Intune están habilitadas y si la aplicación Azure Gateway tiene establecidos los permisos adecuados.
El comando Sh OAuthAction no muestra el estado de OAuth como completo.	Consulte la configuración de DNS y los permisos configurados en la aplicación de Azure Gateway.
El dispositivo Android o iOS no muestra la solicitud de autenticación dual.	Compruebe si el ID de dispositivo de factor dual logonSchema está vinculado al servidor virtual de autenticación.

Estado y condición de error de OAuth de NetScaler Gateway

Estado	Condición de error
AADFORGRAPH	Secreto no válido, URL no resuelta, tiempo de espera de la conexión agotado
MDMINFO	`*manage.microsoft.com`está caído o es inalcanzable
GRAPH	El punto final del gráfico no está accesible
CERTFETCH	No se puede hablar con el token del dispositivo de punto final https://login.microsoftonline.com debido a un error de DNS. Para validar esta configuración, ve a shell y escribe cURL https://login.microsoftonline.com. Este comando debe validarse.

Nota: Cuando el estado de OAuth es correcto, el estado se muestra como COMPLETE.

Mayor compatibilidad con Azure AD Graph

March 27, 2024

Como Azure AD Graph se ha retirado, los clientes que activen una nueva aplicación no pueden usar los permisos anteriores que estaban disponibles con Azure AD Graph. Sin embargo, los clientes con aplicaciones existentes que quieran usar los permisos anteriores de Azure AD Graph durante un

tiempo más pueden seguir haciéndolo realizando algunos cambios de configuración en el dispositivo de puerta de enlace. Esta configuración se admite en NetScaler Gateway versión 13.1-27.xx y versiones posteriores.

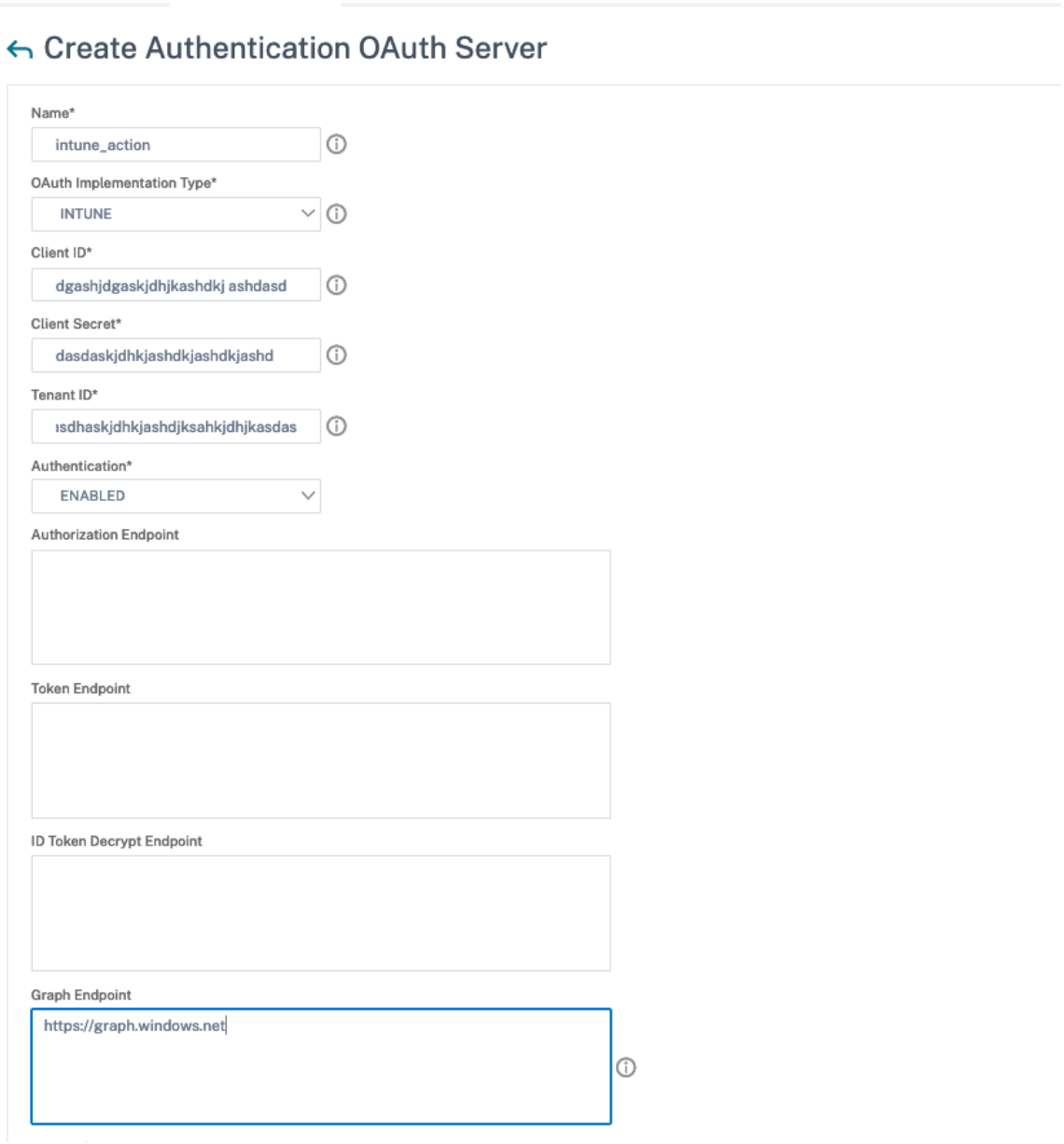
Realice los siguientes cambios de configuración en el dispositivo NetScaler Gateway:

1. En el símbolo del sistema, ejecute el siguiente comando.

```
shell nsapimgr_wr.sh -ys call=”ns_intune_enable_old_endpoints”
<!--NeedCopy-->
```

2. Vaya a **Seguridad > Tráfico de aplicaciones AAA > Directivas > Autenticación > Directivas avanzadas > Acciones > Acciones de OAUTH**.

   a) Seleccione un servidor de OAuth existente.
   b) Haga clic en **Más**.
   c) En **Dispositivo de punto final de Graph**, asegúrese de que la URL se parece a la que se muestra en la ilustración.



Soporte de transporte de datos iluminado por HDX

January 26, 2024

La compatibilidad con Enlightened Data Transport (EDT) para NetScaler Gateway garantiza una experiencia de usuario de alta definición durante la sesión de escritorios virtuales para los usuarios que ejecutan la aplicación Citrix Workspace.

Además, se facilita el cifrado de extremo a extremo con DTLS 1.0 para la terminación de EDT entre la

aplicación Citrix Workspace y el VDA. Para obtener más información, consulte Compatibilidad con el protocolo DTLS.

NetScaler Gateway habilitado para EDT ofrece una buena experiencia de usuario tanto en condiciones de LAN como de WAN. Con EDT, no necesita ninguna configuración administrativa o de usuario cuando se desprende de una a otra. El beneficio es más visible en redes de alta latencia con pérdida moderada de paquetes, donde la experiencia del usuario generalmente se retrasaría con respecto a las alternativas.

Cuándo utilizar el protocolo Enlightened Data Transport

March 27, 2024

En los siguientes casos se ilustra el uso de NetScaler Gateway habilitado para EDT.

- Un usuario quiere disfrutar de una experiencia tan buena como en un entorno LAN mientras accede de forma remota a los recursos empresariales.
- Un usuario quiere una experiencia de usuario de escritorio y aplicaciones virtuales enriquecidas en redes Wi-Fi y móviles en las que la calidad de la red es deficiente debido a la congestión, la alta pérdida de paquetes y la alta latencia.

Los siguientes puntos deben tenerse en cuenta al utilizar EDT.

- El mando DTLS en el nivel del servidor virtual está habilitado de forma predeterminada.
- No se admite IPv6 con DTLS.
- El dispositivo ahora se puede configurar para la funcionalidad de doble salto para el tráfico de EDT entre Receiver y VDA. Para obtener más información, haga clic en Implementación en una DMZ de doble salto.

Nota: EDT es compatible con la plataforma MPX FIPS en la versión 12.1, compilación 49.xx y versiones posteriores. En los dispositivos MPX basados en el chip SSL Intel Coleto, EDT es compatible con la versión 12.1 versión 51.16 y versiones posteriores.

Configurar NetScaler Gateway para que admita Enlightened Data Transport y HDX Insight

March 27, 2024

El tráfico de EDT a través de Gateway ahora tiene visibilidad de extremo a extremo. La disponibilidad de datos de visibilidad histórica y en tiempo real permite a NetScaler ADM admitir una amplia variedad de casos de uso.

Se admiten los siguientes casos:

Escenario	Compatibilidad con EDT
NetScaler Gateway	Sí
NetScaler Gateway con alta disponibilidad (HA)	Sí
Optimización de NetScaler Gateway con alta disponibilidad (HA)	Sí
NetScaler con Unified Gateway	Sí
NetScaler Gateway con GSLB	Sí
NetScaler Gateway con clúster	Sí
Cifrado DTLS de la aplicación Citrix Workspace a NetScaler Gateway	Sí
Secure Tíquet Authority dobles (STA) en NetScaler Gateway	Sí
Tiempo de espera de sesión ICA de NetScaler Gateway	Sí
ICA multisecuencia de NetScaler Gateway	No
Fiabilidad de la sesión de NetScaler Gateway (puerto 2598)	Sí
Doble salto de NetScaler Gateway	Sí
Cifrado DTLS de NetScaler a VDA	Sí
HDX Insight	Sí
NetScaler Gateway en el modo de IPv6	No
SOCKS de NetScaler Gateway (puerto 1494)	No
Proxy LAN puro de NetScaler (consulte la nota)	No

> **Nota:**
>
> No se admite EDT si el proxy LAN de NetScaler está configurado en el modo de usuario de LAN o en el modo transparente. Sin embargo, se admite TCP. Para obtener más información, consulte:
>
> - Configuración del proxy ICA saliente

- Recopilación de análisis de HDX Insight para usuarios de LAN con NetScaler mediante SOCKS

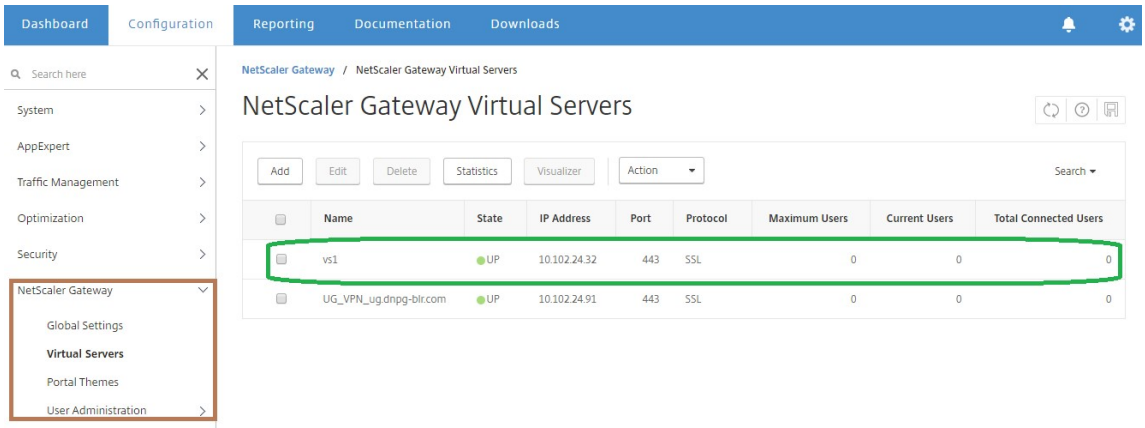
Configurar NetScaler Gateway para admitir el Enlightened Data Transport

Si utiliza el Enlightened Data Transport (EDT), la Transport Layer Security de datagramas (DTLS) debe estar habilitada para cifrar la conexión UDP utilizada por EDT. El parámetro DTLS debe estar habilitado en el nivel del servidor virtual de VPN de puerta de enlace. Además, los componentes de Citrix Virtual Apps and Desktops deben actualizarse y configurarse correctamente para conseguir tráfico cifrado entre el servidor virtual de VPN de puerta de enlace y el dispositivo del usuario.

> **Nota:** El puerto UDP (por ejemplo, el puerto 443) configurado para el servidor virtual front-end de NetScaler Gateway debe abrirse en la DMZ para que el servidor virtual reciba las conexiones DTLS. DTLS y CGP son requisitos previos para que EDT sea compatible con NetScaler Gateway.

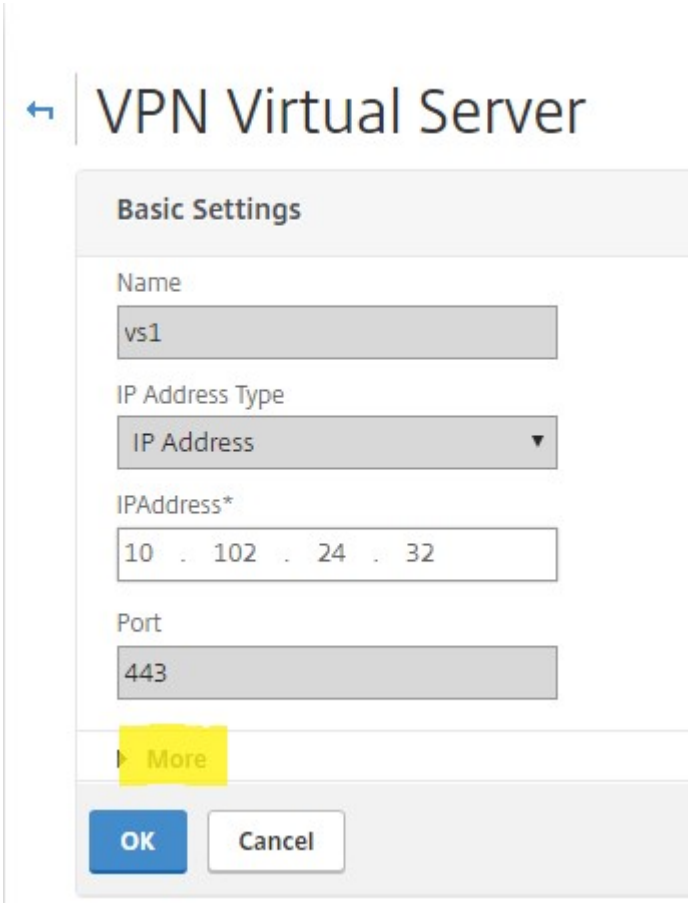
Para configurar NetScaler Gateway para que admita EDT mediante GUI

1. Implemente y configure NetScaler Gateway para comunicarse con StoreFront y autenticar a los usuarios de Citrix Virtual Apps and Desktops.
2. En la ficha Configuración de la GUI de NetScaler, expanda **NetScaler Gateway** y seleccione **Servidores virtuales**.



3. Haga clic en **Modificar** para mostrar la configuración básica del servidor virtual de VPN y, a continuación, compruebe el estado de la configuración DTLS.

4. Haga clic en **Más** para mostrar otras opciones de configuración.



5. Seleccione **DTLS** para proporcionar seguridad en las comunicaciones de los protocolos de datagramas. Haga clic en **Aceptar**. El área **Configuración básica** del servidor virtual de VPN muestra que el indicador DTLS está establecido en **True**.

Para configurar la compatibilidad con NetScaler Gateway para EDT mediante CLI

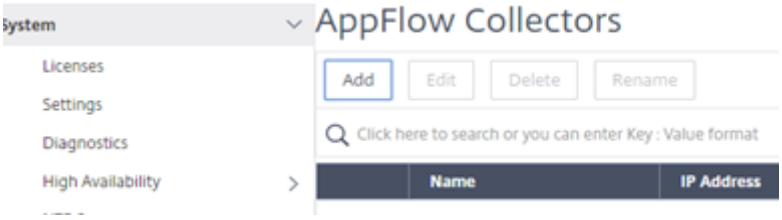
```
set vpn vserver vs1 -DTLS ON
```

Configurar NetScaler Gateway para admitir HDX Insight

HDX Insight proporciona visibilidad integral del tráfico HDX a las aplicaciones y escritorios virtuales que pasan por NetScaler. También permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento.

Para configurar NetScaler Gateway para que admita HDX Insight mediante la interfaz gráfica de usuario

1. En la ficha **Configuración**, vaya a **Sistema> AppFlow>Collectors** y haga clic en **Agregar**.



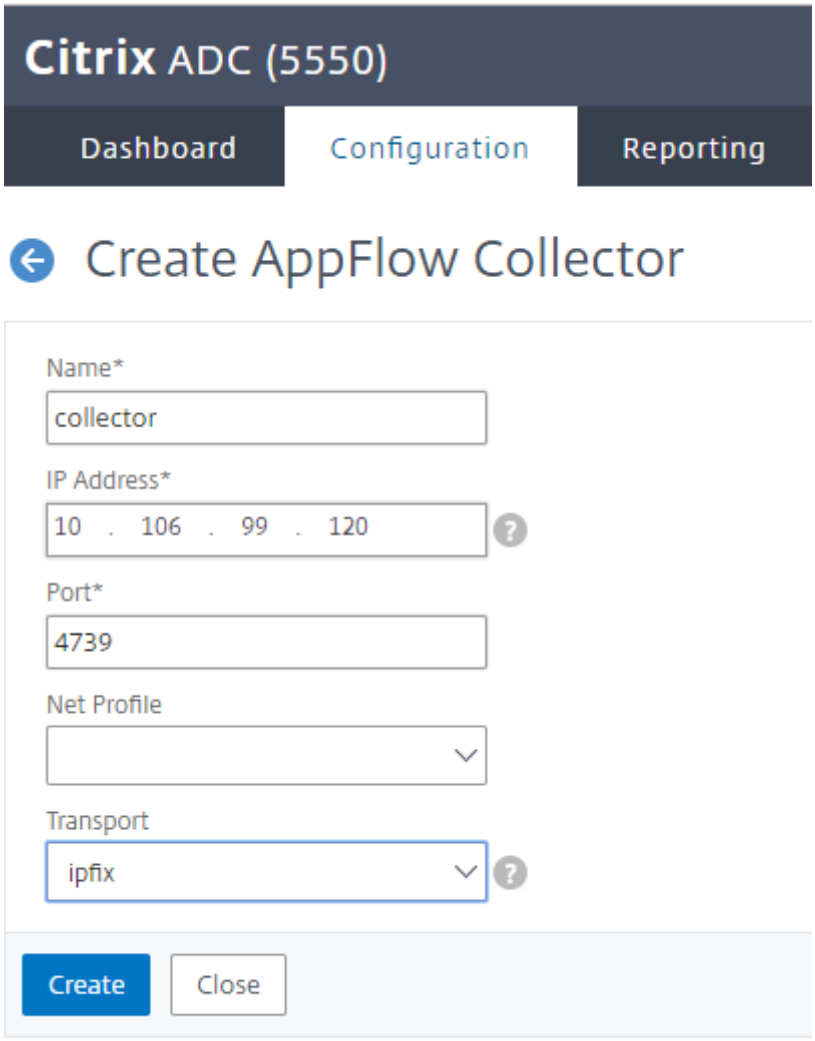
2. En la página **Crear recopilador de AppFlow**, rellene los campos siguientes y haga clic en **Crear**.
   Nombre: nombre del coleccionista

   Dirección IP: dirección IPv4 del recopilador

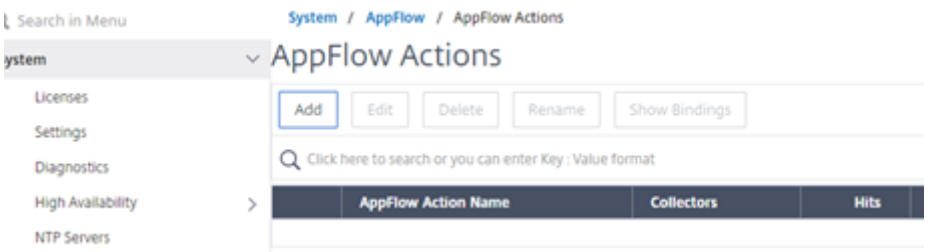
   Puerto: puerto en el que escucha el recopilador

Perfil de red: perfil de red que se va a asociar con el recopilador. La dirección IP definida en el perfil se utiliza como dirección IP de origen para el tráfico de AppFlow de este recopilador. Si no establece este parámetro, la dirección IP de NetScaler (NSIP) se utiliza como dirección IP de origen.

Transporte: tipo de colector de transporte.



3. Vaya a **Sistema > AppFlow> Acciones**y haga clic en **Agregar**.



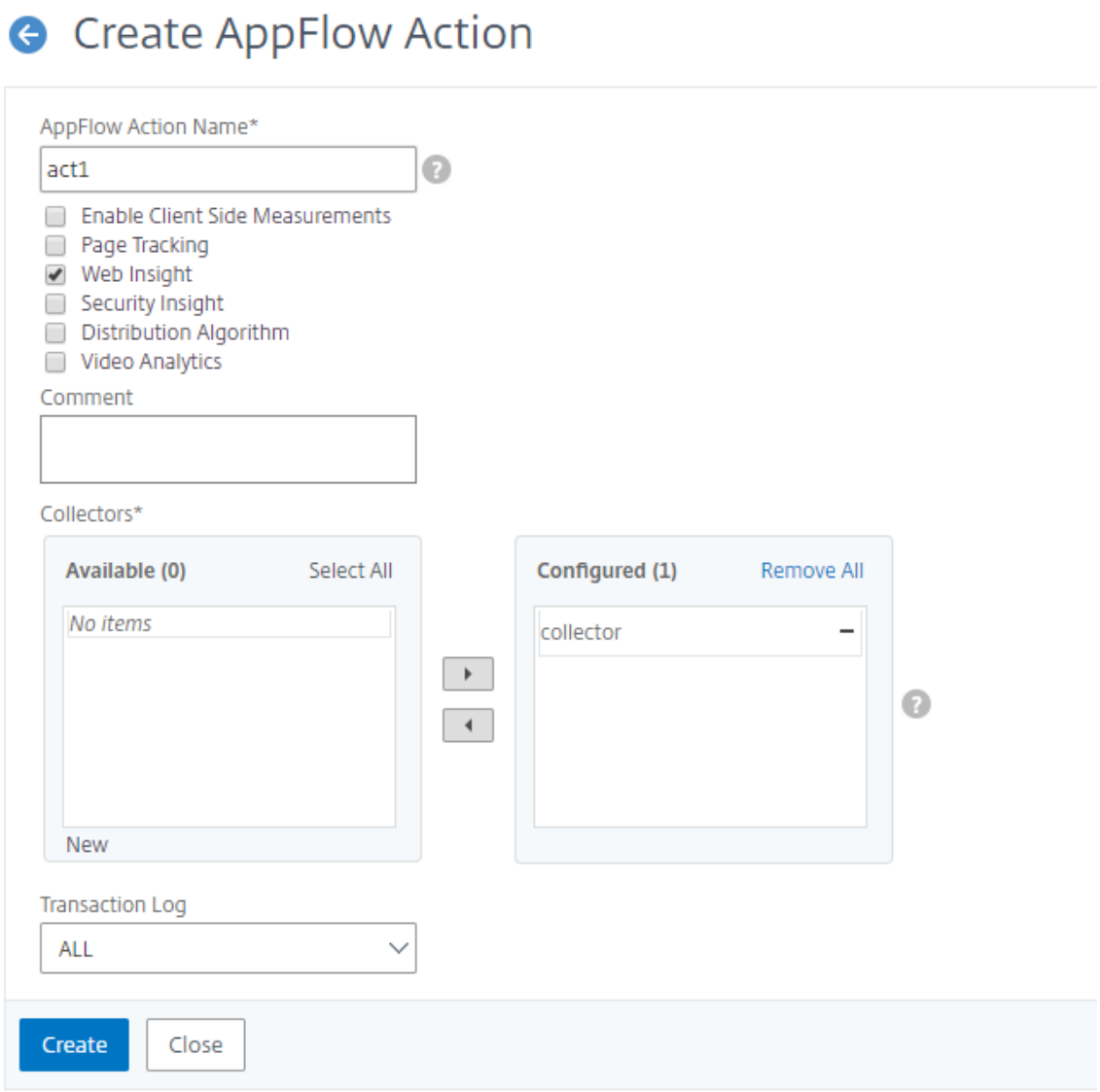
4. En la página **Crear acción de AppFlow**, rellene los campos siguientes y haga clic en **Crear**.

Nombre de acción de AppFlow: nombre de la acción

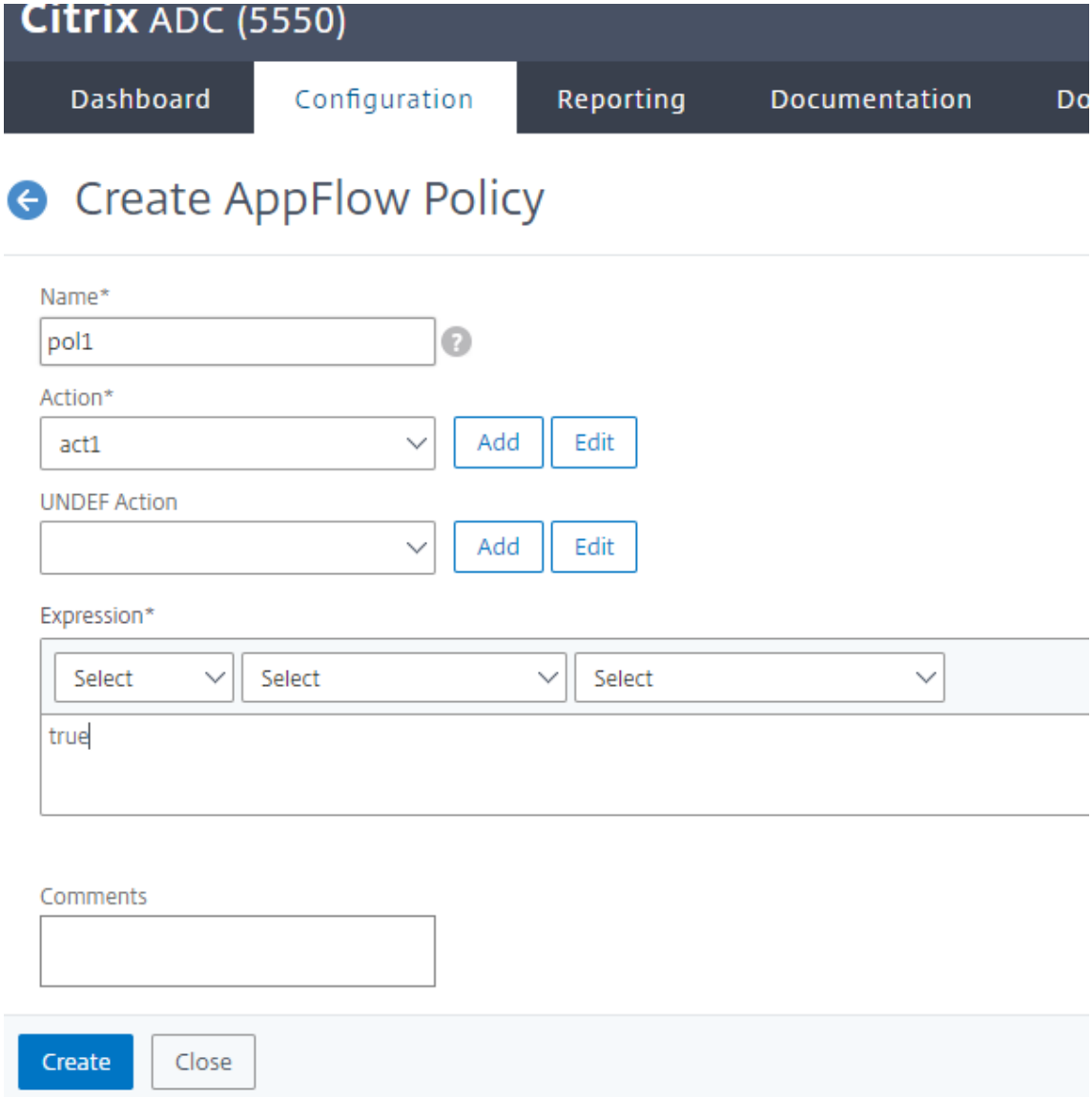
Comentario: cualquier comentario sobre la acción

Collector: seleccione los nombres de los recopiladores que se van a asociar a la acción de AppFlow.

Registro de transacciones: tipo de transacciones que se van a registrar.



5. Vaya a **Sistema> AppFlow>Directivas**y haga clic en **Agregar**.



6. En la página **Crear directiva de flujo de aplicaciones**, rellene los siguientes campos y haga clic en **Crear**.

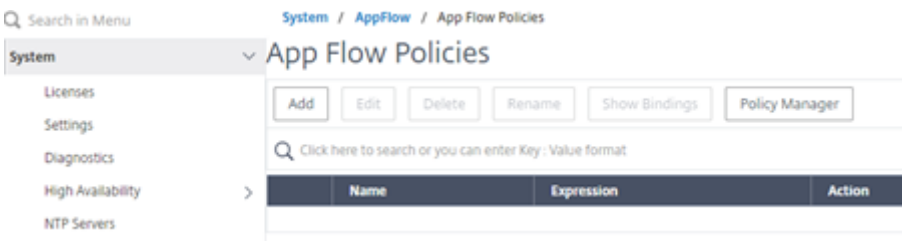
   Nombre: nombre de la directiva.

   Acción: nombre de la acción que se va a asociar a la directiva.

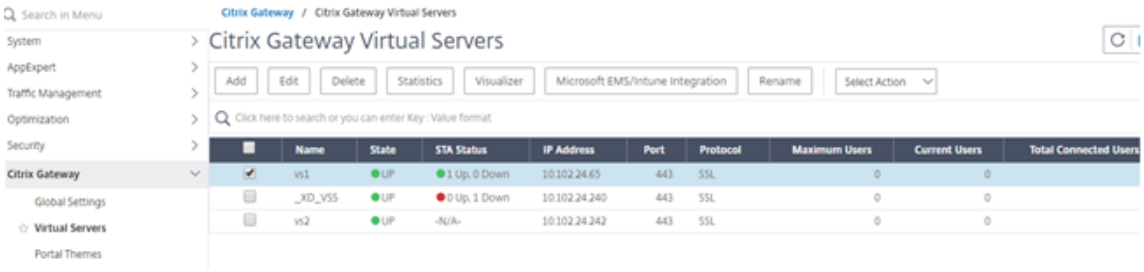
   UNDEF: nombre de la acción de AppFlow que se va a asociar a esta directiva cuando se produce un evento no definido.

   Expresión: expresión u otro valor con el que se evalúa el tráfico. Debe ser una expresión booleana.

   Comentarios: cualquier comentario sobre esta directiva.

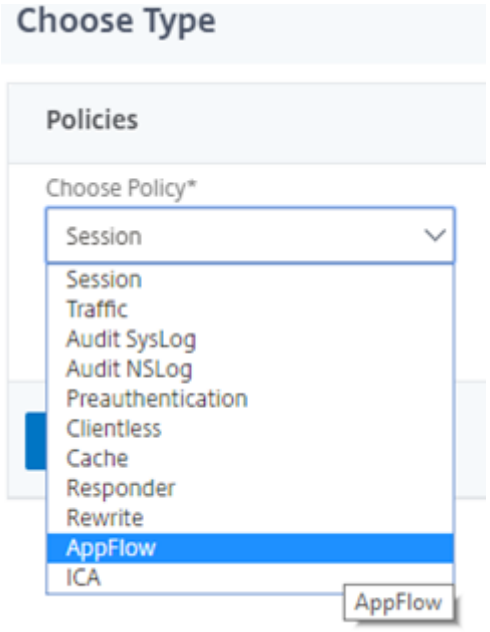


7. Vaya a **NetScaler Gateway>Servidores virtuales**, seleccione el servidor virtual y haga clic en **Modificar**.

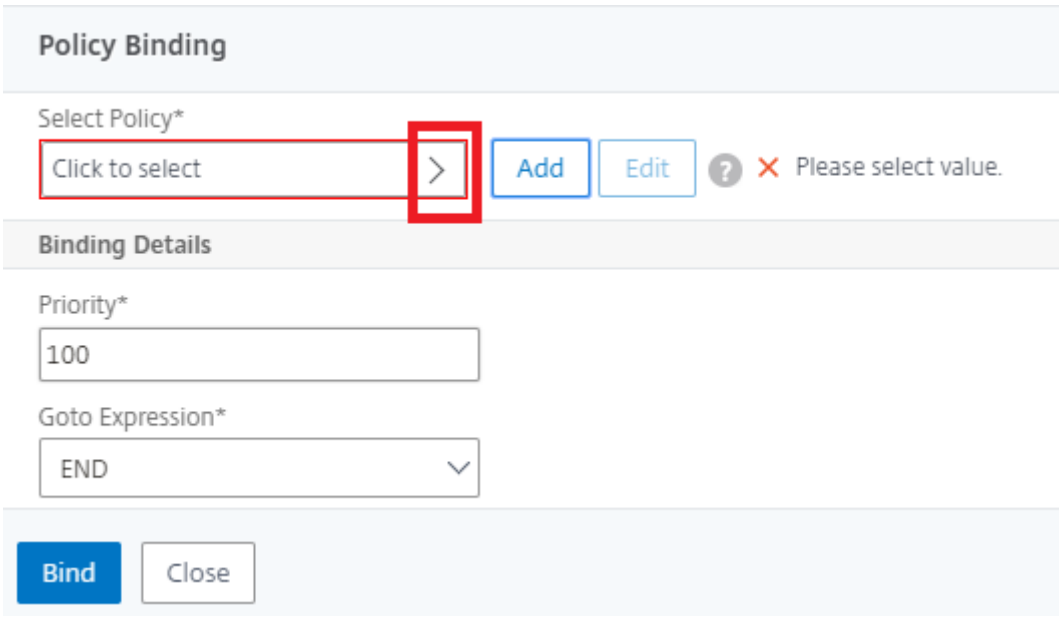


8. Desplácese hacia abajo en la página **Servidor Virtual VPN** y, en la sección **Directivas**, haga clic en **+**.

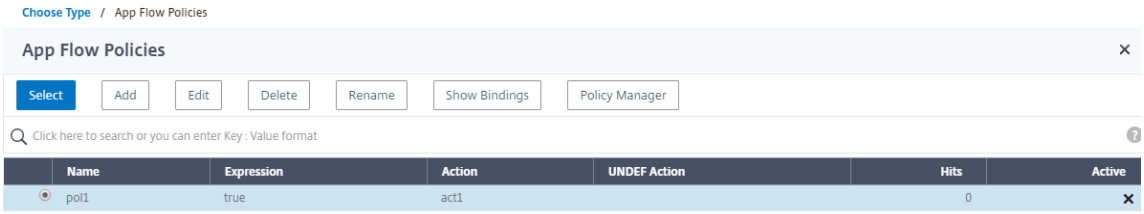
9. En la pantalla **Elegir tipo**, en el menú desplegable **Elegir directiva**, seleccione **AppFlow**. En el menú desplegable **Elegir tipo**, elija **Solicitud o SolicitudICA**y haga clic en**Continuar**.



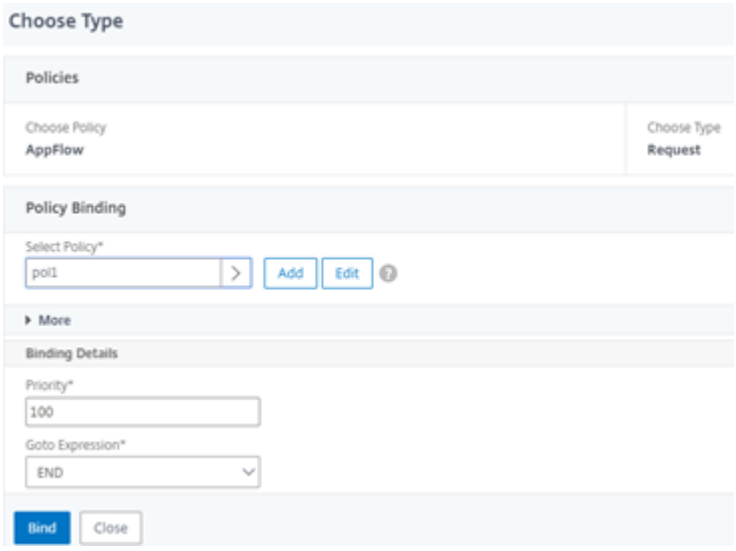
10. Haga clic en la flecha resaltada en **Seleccionar directiva**.



11. Seleccione la **directiva AppFlow** y haga clic en **Seleccionar**.



12. Por último, haga clic en **Vincular**.



Para configurar la compatibilidad con NetScaler Gateway para HDX Insight mediante la CLI, escriba el siguiente comando

```
add appflow collector col3 -IPAddress<ip_mas>
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
    type <ICA_Request>
```

Inhabilitar HDX Insight para sesiones HDX que no sean de NSAP

En un dispositivo NetScaler, ahora puede inhabilitar HDX Insight para las sesiones HDX que no sean de NSAP HDX.

En la línea de comandos, escriba:

```
set ica parameter HDXInsightNonNSAP (YES | NO )
<!--NeedCopy-->
```

De forma predeterminada, la sesión HDX Insight para no NSAP está habilitada.

Descubrimiento de PMTUD y propagación de bits DF para EDT a través de NetScaler Gateway

March 27, 2024

A partir de la versión 13.1 compilación 17.x, el dispositivo NetScaler Gateway admite la aplicación de bits DF para la detección de unidades de transmisión máxima (PMTUD) de ruta de EDT. El descubrimiento de MTU de ruta ayuda a determinar dinámicamente la unidad de transmisión máxima (MTU) cuando se establece una sesión. La aplicación de bits DF evita la fragmentación de EDT que puede provocar una degradación del rendimiento o la imposibilidad de establecer una sesión.

En versiones anteriores, NetScaler Gateway admitía MTUD de ruta EDT, pero no admitía la aplicación de bits DF.

Para obtener más información, consulte Descubrimiento de MTU de EDT.

Habilitar la función de PMTUD mediante la CLI

En la línea de comandos, escriba;


```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-
    HDXInsightNonNSAP ( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )]
     [-EDTPmtudDFTimeout <positive_integer>] [-L7LatencyFrequency <
    positive_integer>]
<!--NeedCopy-->
```

Ejemplo:

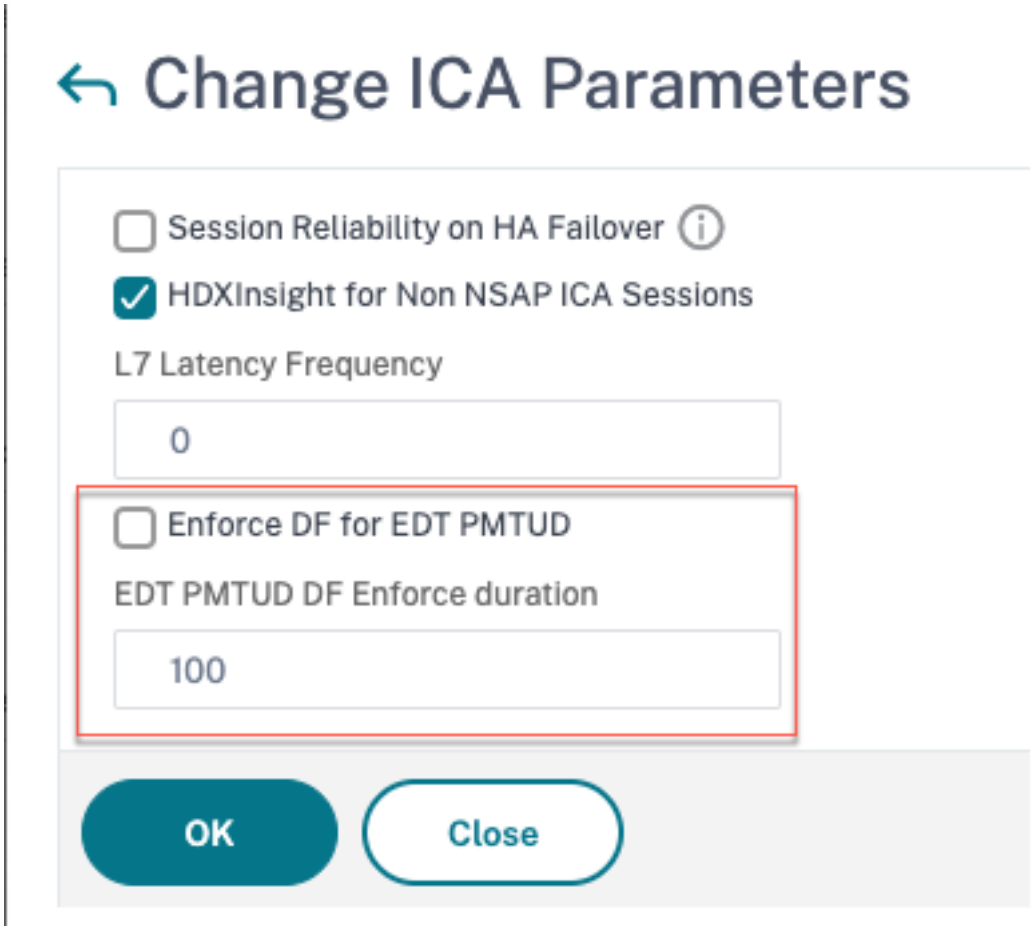
```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED -
    EDTPmtudDFTimeout 100
<!--NeedCopy-->
```

> **Nota:**
>
> A partir de la versión 13.1, compilación 42.x y versiones posteriores, el parámetro EDTPmtudDF está habilitado de forma predeterminada. Anteriormente, esta opción estaba inhabilitada de forma predeterminada.

Habilitar la función de PMTUD mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Configuración > Cambiar parámetros ICA**.
2. En **EDT PMTUD DF Enforce duration**, introduzca el tiempo de espera en segundos para la aplicación PMTUD DF.

> **Nota:**
>
> A partir de la versión 13.1, compilación 42.x y versiones posteriores, la opción **Enforce DF para EDT PMTUD** está habilitada de forma predeterminada. Anteriormente, esta opción estaba inhabilitada de forma predeterminada.



Umbral de latencia L7

March 27, 2024

La función de umbral de latencia L7 de HDX Insight detecta de forma activa los problemas de latencia de red de extremo a extremo a nivel de aplicación y toma medidas proactivas. La función de umbral de latencia L7 realiza una supervisión de latencia en tiempo real para detectar los picos y envía notificaciones a HDX Insight si la latencia supera la latencia mínima observada.

Anteriormente, los valores promedio de latencia L7 del lado del cliente y del servidor se enviaban cada 60 segundos a HDX Insight. Cualquier pico observado dentro de este intervalo se promedió y, por lo tanto, permaneció sin ser detectado. Además, no había monitorización de latencia en vivo para detectar estos picos.

En qué se diferencia la latencia L7 de la latencia L4

Las latencias de red también se capturan y muestran en el nivel L4. Estas latencias se calculan a partir de la capa TCP y no requieren análisis del tráfico ICA. Por lo tanto, son relativamente fáciles de obtener y consumen menos CPU. Sin embargo, el principal inconveniente de la latencia L4 es comprender la latencia de extremo a extremo. Si hay proxies TCP en la ruta, la latencia L4 captura solo la latencia del NetScaler al proxy TCP. Esto puede dar lugar a información incompleta y, por lo tanto, provocar dificultades para depurar el problema.

La latencia de L7 se calcula analizando el tráfico ICA. El cálculo de latencia L7 se realiza en la capa ICA y, por lo tanto, los proxies intermedios no producen valores de latencia incompletos. Por lo tanto, proporciona detección de latencia de extremo a extremo.

En las ilustraciones siguientes se muestra un tipo de implementación con y sin proxy TCP.

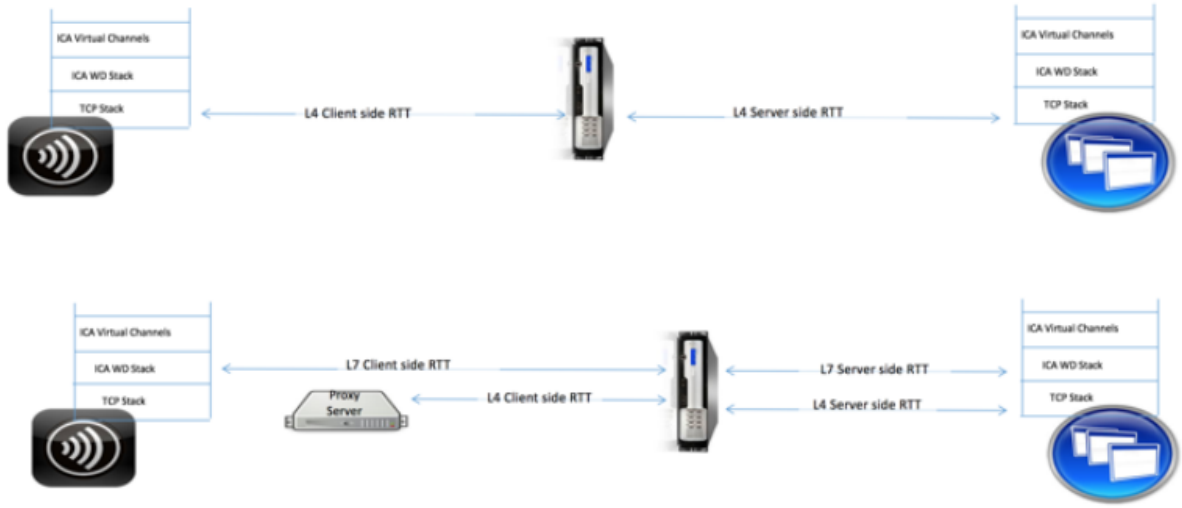


Fig 2. Deployment with TCP Proxies

Diferencia entre los cálculos de latencia ICA RTT y L7

ICA RTT representa el tiempo total de ida y vuelta desde la aplicación Citrix Workspace hasta Virtual Delivery Agent (VDA). La latencia de L7 proporciona detalles detallados sobre las latencias del lado del cliente y del servidor. La latencia del cliente L7 es la latencia entre la aplicación Citrix Workspace y NetScaler Gateway. La latencia del servidor L7 es la latencia entre NetScaler Gateway y VDA.

> **Nota: El**cálculo de latencia L7 del servidor para el servidor solo se admite para las versiones 7.13 y versiones posteriores de Citrix Virtual Apps and Desktops.

Configurar el umbral de latencia de L7 mediante la CLI

1. Agregue un perfil de latencia ICA.

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
     <positive_integer>] [-l7LatencyMaxNotifyCount <
    positive_integer>]
<!--NeedCopy-->
```

2. Agregue una acción ICA.

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. Agregue una directiva ICA.

```
add ica policy <name> -rule <expression> -action <string> [-
    comment<string>] [-logAction <string>
<!--NeedCopy-->
```

4. Enlazar la directiva ICA al servidor VPN o al punto de enlace global ICA.

```
bind ica global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>] [-type (
    ICA_REQ_OVERRIDE | ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```

O bien

```
bind vpn vserver <name> -policy <string>  [-priority <
    positive_integer>]
<!--NeedCopy-->
```

O bien

```
bind cr vserver <name> -policy <string> [-priority <positive
    _integer>]
<!--NeedCopy-->
```

Argumentos

- **Monitorización de latencia**: Parámetro para habilitar o inhabilitar la supervisión de umbral L7. Cuando este parámetro está habilitado, las notificaciones se envían a HDX Insight cuando se cumplen las condiciones establecidas.

  Valor predeterminado: DESACTIVADO

- **latencyThresholdFactor**: Factor por el cual la latencia activa debe ser mayor que la latencia mínima observada para concluir que se ha superado el umbral y, por lo tanto, debe enviarse una notificación a HDX Insight.

  Valor predeterminado: 4

  Valor mínimo: 2

  Valor máximo: 65535

- **latencyWaitTime**: Tiempo en segundos para que el dispositivo espere una vez superado el umbral de latencia para enviar una notificación a HDX Insight.

  Valor por defecto: 20

  Valor mínimo: 1

  Valor máximo: 65535

- **latencyNotifyInterval**: Intervalo de tiempo en segundos para que el dispositivo envíe notificaciones posteriores a HDX Insight una vez transcurrido el tiempo de espera.

  Valor por defecto: 20

  Valor mínimo: 1

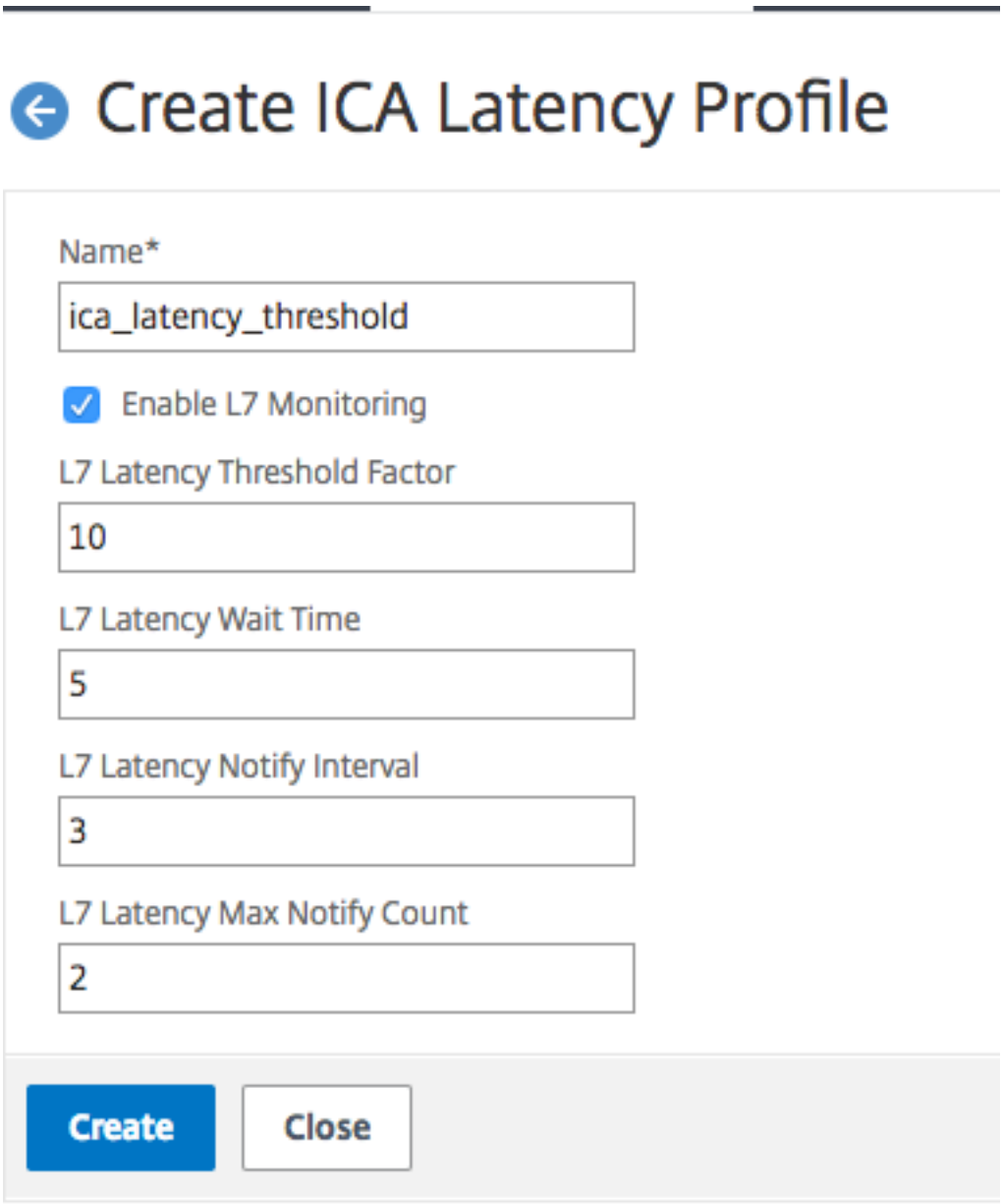
  Valor máximo: 65535

- **LatencyMaxNotifyCount**: Número máximo de notificaciones que se pueden enviar a HDX Insight dentro de un intervalo en el que la latencia está por encima del umbral.

  Valor predeterminado: 5

Configurar el umbral de latencia de L7 mediante la GUI

1. Vaya a **Configuración** > **NetScaler Gateway** > **Directivas** > **ICA**.
2. Seleccione la ficha **Perfiles de latencia ICA** y haga clic en **Agregar**.
3. En la página **Crear Perfil de Latencia ICA**, realice lo siguiente.



- Seleccione Supervisión de **latencia de L7 para habilitar la supervisión** del umbral de nivel 7.
- En **Factor de umbral L7**, introduzca el valor en el que la latencia activa debe superar la latencia mínima observada para enviar notificaciones a HDX Insight.
- En **Tiempo de espera de latencia de L7**, introduzca el tiempo en segundos que debe esperar el dispositivo después de superar el umbral para enviar una notificación a HDX Insight.
- En **Intervalo de notificación de latencia de nivel 7**, introduzca el tiempo en segundos para que el dispositivo envíe notificaciones posteriores a HDX Insight una vez transcurrido el tiempo de espera.

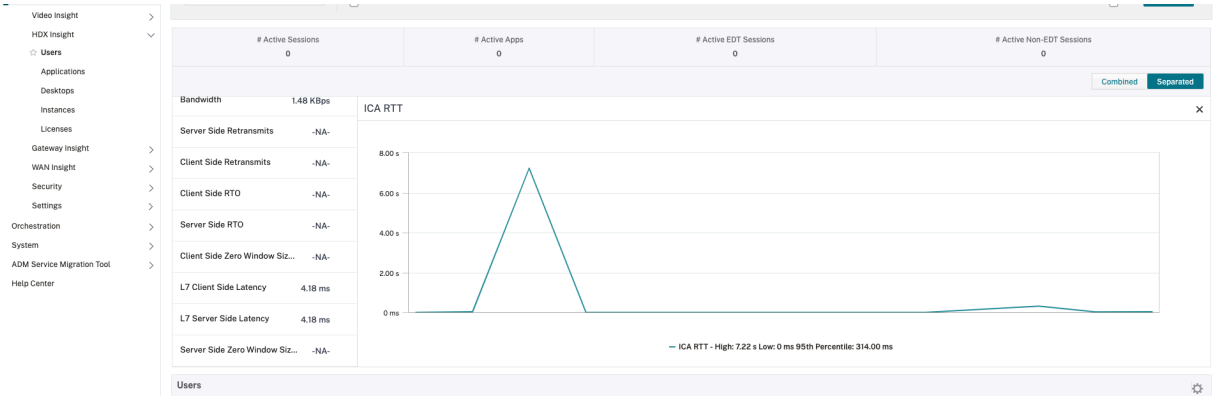
- En **Recuento máximo de notificaciones de latencia de nivel 7**, introduzca el número máximo de notificaciones que se pueden enviar a HDX Insight en un intervalo en el que la latencia esté por encima del umbral.
  Nota: El recuento máximo de notificaciones de latencia L7 se aplica una vez que se supera el umbral y se restablece cuando la latencia activa cae por debajo del umbral. La periodicidad de estas notificaciones se rige por el intervalo de notificación.

4. Haga clic en **Crear**.

> **Importante:**
>
> Después de configurar los parámetros del umbral de latencia de L7, debe configurar HDX Insight. Para obtener más información, consulte Configurar NetScaler Gateway para que sea compatible con HDX Insight.

Ver parámetros de latencia de nivel 7 en NetScaler ADM

Para ver los parámetros de latencia de L7 en NetScaler ADM, vaya a **Analytics > HDX Insight > Aplicaciones** o **análisis > HDX Insight > Usuarios**.

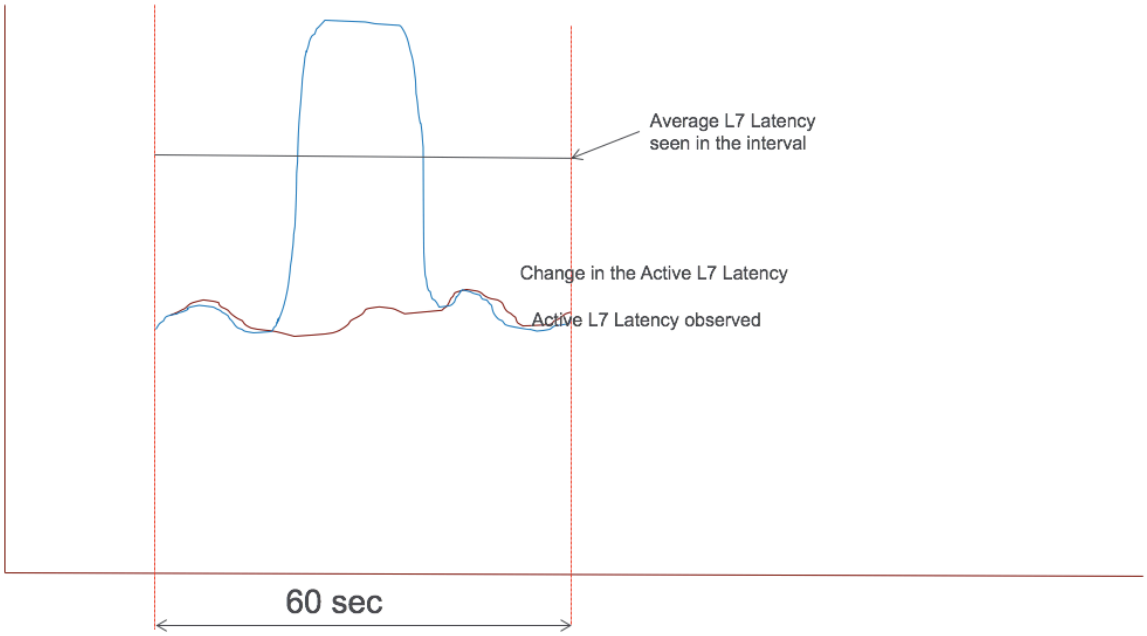


El modelo de medición de latencia L7 frente al modelo de informes de umbral de latencia L7

El modelo de medición de latencia L7

En el módulo de medición de latencia L7, los valores medios de latencia L7 del lado del cliente y del servidor se envían a HDX Insight cada 60 segundos. Como resultado, los picos observados dentro de este intervalo se promedian y, por lo tanto, no se detectan. Además, el módulo de medición de latencia L7 no tiene la capacidad de supervisión de latencia en vivo.

En la siguiente ilustración se ilustra un modelo de medición de latencia L7 de muestra.

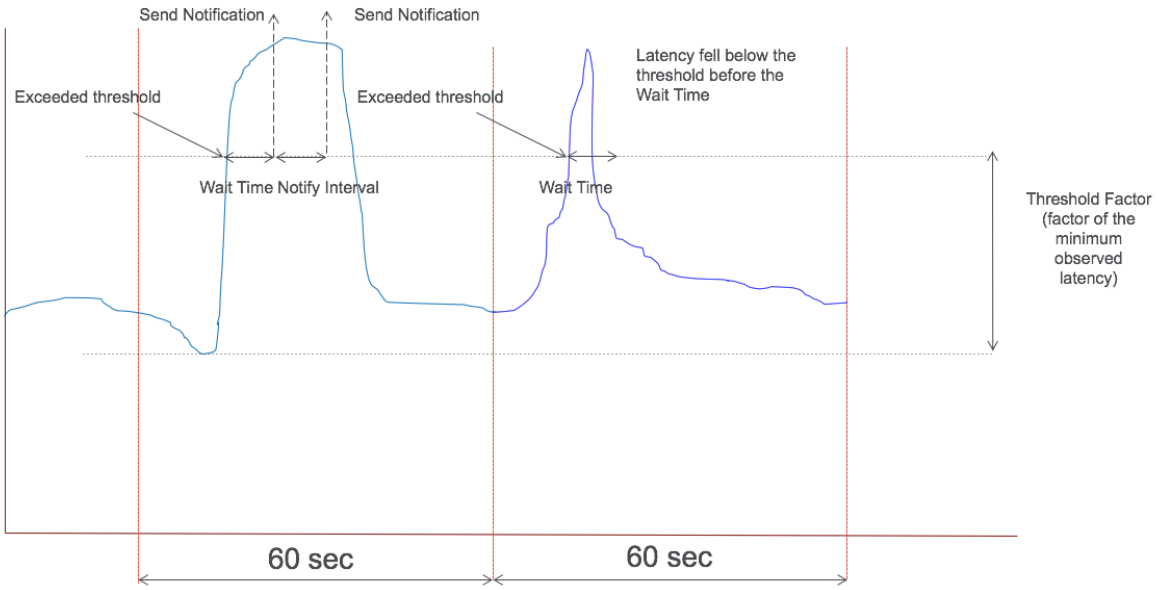


Modelo de informes de umbral de latencia de nivel 7

El modelo de informes de umbral de latencia L7 tiene la capacidad de monitorización de latencia en tiempo real para detectar picos. Las notificaciones se envían a HDX Insight si la latencia supera la latencia mínima observada.

Cuando se supera un factor de umbral, se detecta el aumento de la latencia. Una vez que expira el tiempo de espera del umbral configurado, se envía una notificación a HDX Insight. Se envía una notificación posterior a HDX Insight después de que haya expirado el tiempo de espera y se supere el factor umbral.
En caso de que el valor de latencia caiga por debajo del factor umbral antes de que expire el tiempo de espera, no se envía ninguna notificación a HDX Insight.

En la siguiente ilustración se ilustra un modelo de informe de umbral de latencia de nivel 7 de muestra.



Los siguientes parámetros se pueden configurar en tiempo de ejecución:

- Supervisión de umbrales (ACTIVAR/DESACTIVAR)
- Factor umbral
- Tiempo de espera umbral
- Intervalo de notificación
- Recuento máximo de notificaciones

Reductor para HDX

March 27, 2024

Reducer for HDX es un compresor de uso general administrado por Citrix Virtual Apps and Desktops que funciona en todos los canales virtuales.

Las versiones 14.1—8.50 de NetScaler Gateway y posteriores admiten la versión más reciente del reductor para HDX. El reductor más reciente mejora el rendimiento general de NetScaler Gateway con las siguientes capacidades:

- Reduce la utilización del ancho de banda de la red para las sesiones ICA.
- Proporciona una respuesta más rápida, ya que los paquetes tardan menos en transmitirse.

Para obtener detalles sobre cómo usar el reductor más reciente, consulte Cómo usar el nuevo reductor.

Las siguientes versiones de software son compatibles con el reductor más reciente.

- Citrix Virtual Apps and Desktops 7 2303 (Windows) y versiones posteriores.
- Aplicación Citrix Workspace 2303 (Windows) y versiones posteriores.

> **Nota:**
>
> Si utiliza las versiones 2311 (Windows) de la aplicación Citrix Workspace 2311 (Windows) y Citrix Virtual Apps and Desktops 7 2311 (Windows), el reductor más reciente está habilitado de forma predeterminada.

En la siguiente tabla se describe el estado de los inicios de las sesiones ICA y la información sobre HDX con el reductor más reciente, en la versión 14.1 de NetScaler Gateway.

Último reductor	NetScaler Gateway 14.1
Negociación de reductores más reciente e información sobre NSAP HDX	El inicio de la conexión ICA se ha realizado correctamente. Es compatible con HDX Insight.
Negociación de reductores más reciente + NSAP HDX insight + SmartControl	El inicio de la conexión ICA se ha realizado correctamente. Es compatible con HDX Insight.
Negociación de reductores más reciente e información sobre HDX que no es de NSAP	El inicio de la conexión ICA se ha realizado correctamente. No se admite HDX insight.

> **Nota:**
>
> NetScaler Gateway 13.1 y las versiones anteriores no admiten HDX Insight y SmartControl con el reductor más reciente.

Para obtener más información sobre la configuración de HDX Insight, consulte Configurar NetScaler Gateway para que sea compatiblecon HDX Insight.

Proxy RDP

March 27, 2024

La funcionalidad del proxy RDP se proporciona como parte de NetScaler Gateway. En una implementación típica, el cliente RDP se ejecuta en el equipo de un usuario remoto. El dispositivo NetScaler Gateway se implementa en la DMZ y la comunidad de servidores RDP se encuentra en la red corporativa interna.

El usuario remoto;

1. se conecta a la dirección IP pública de NetScaler Gateway

2. establece una conexión VPN SSL
3. autentica
4. accede a los escritorios remotos a través del dispositivo NetScaler Gateway

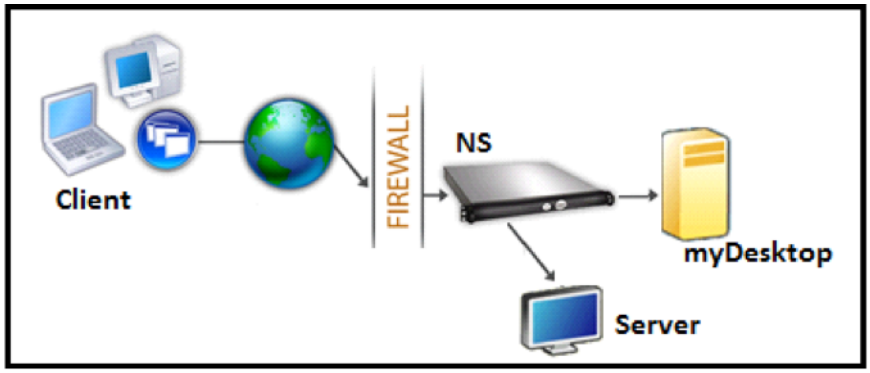
La función de proxy RDP se admite en los modos VPN sin cliente y proxy ICA.

> **Nota:**
>
> NetScaler Gateway no admite las aplicaciones Remote Desktop Session Host (RDSH), Remote App, RDS multiusuario, RDP ni RDP.

Las siguientes funciones del proxy RDP proporcionan acceso a una comunidad de escritorios remotos a través de NetScaler Gateway.

- Proteja el tráfico RDP mediante VPN sin cliente o modo Proxy ICA (sin túnel completo).
- SSO (inicio de sesión único) en servidores RDP a través de NetScaler Gateway. También proporciona una opción para inhabilitar el SSO si es necesario.
- Función de cumplimiento (SmartAccess), en la que los administradores de NetScaler pueden inhabilitar determinadas capacidades de RDP mediante la configuración de NetScaler Gateway.
- Solución de puerta de enlace única o sin estado (doble) para todas las necesidades (VPN/ICA/RDP/Citrix Endpoint Management).
- Compatibilidad con el cliente MSTSC nativo de Windows para RDP sin necesidad de clientes personalizados.
- Uso del cliente RDP existente proporcionado por Microsoft en MACOSX, iOS y Android.

En la siguiente ilustración se muestra una descripción general de la implementación:



Implementación mediante VPN sin cliente

En este modo, los vínculos RDP se publican en la página de inicio o portal de Gateway, como marcadores, a través de la configuración de `add vpn url` o mediante un portal externo. El usuario puede hacer clic en estos vínculos para obtener acceso al Escritorio remoto.

Implementación mediante ICA Proxy

En este modo, se configura una página principal personalizada en el VIP de puerta de enlace mediante el parámetro `wihome`. Esta página principal se puede personalizar con la lista de recursos de escritorio remoto a los que el usuario puede acceder. Esta página personalizada se puede alojar en NetScaler o, si es externa, puede ser un iFrame en la página del portal Gateway existente.

En cualquiera de los dos modos, después de que el usuario haga clic en el enlace o icono de RDP aprovisionado, llega a NetScaler Gateway una solicitud HTTPS del recurso correspondiente. La puerta de enlace genera el contenido del archivo RDP para la conexión solicitada y lo envía al cliente. Se invoca el cliente RDP nativo y se conecta a un agente de escucha RDP en Gateway. Gateway realiza el SSO en el servidor RDP mediante la compatibilidad con la aplicación (SmartAccess). La puerta de enlace bloquea el acceso de los clientes a determinadas funciones de RDP, según la configuración de NetScaler y, a continuación, envía el tráfico RDP entre el cliente RDP y el servidor.

Detalles de ejecución

El administrador de NetScaler puede configurar determinadas capacidades de RDP mediante la configuración de NetScaler Gateway. NetScaler Gateway proporciona la función "cumplimiento de RDP"para parámetros importantes de RDP. NetScaler garantiza que el cliente no pueda habilitar los parámetros bloqueados. Si los parámetros bloqueados están habilitados, la función de aplicación RDP sustituye a los parámetros habilitados por el cliente y no se respetan.

> **Importante:** La función de cumplimiento solo se aplica si el SSO está habilitado.

Parámetros RDP compatibles para la aplicación

Se admite la aplicación de los siguientes parámetros de redirección. Estos parámetros se pueden configurar como parte de un perfil de cliente RDP.

- Redirección del portapapeles
- Redirección de impresoras
- Redirección de unidades de disco
- Redirección de puertos COM
- Redirección de dispositivos PNP

Flujo de conexión

El flujo de conexión se puede dividir en dos pasos:

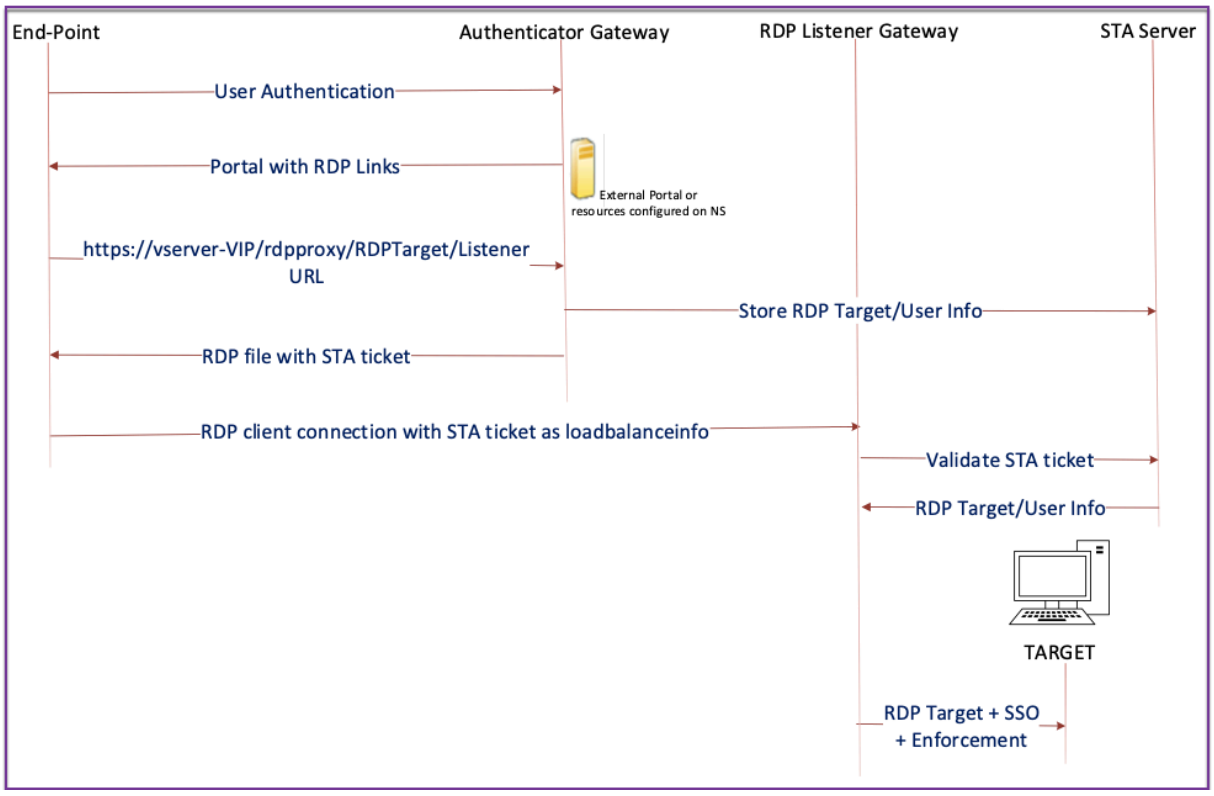
- Enumeración de recursos RDP y descarga de archivos RDP.
- Inicio de la conexión RDP.

Según el flujo de conexión anterior, existen dos soluciones de implementación:

- Solución de puerta de enlace sin estado (doble): la enumeración de recursos RDP y la descarga de archivos RDP se realizan a través de la puerta de enlace del autenticador, pero el inicio de la conexión RDP se realiza a través de la puerta de enlace de escucha de
- Solución de gateway única: la enumeración de recursos RDP, la descarga de archivos RDP y el inicio de la conexión RDP se realizan a través de la misma puerta de enlace.

Compatibilidad con gateway sin estado (dual)

En la siguiente ilustración se muestra la implementación:



- Un usuario se conecta a la VIP de puerta de enlace de autenticación y proporciona las credenciales.
- Tras iniciar sesión correctamente en la puerta de enlace, se redirige al usuario a la página principal o al portal externo, que enumera los recursos de escritorio remoto a los que puede acceder el usuario.

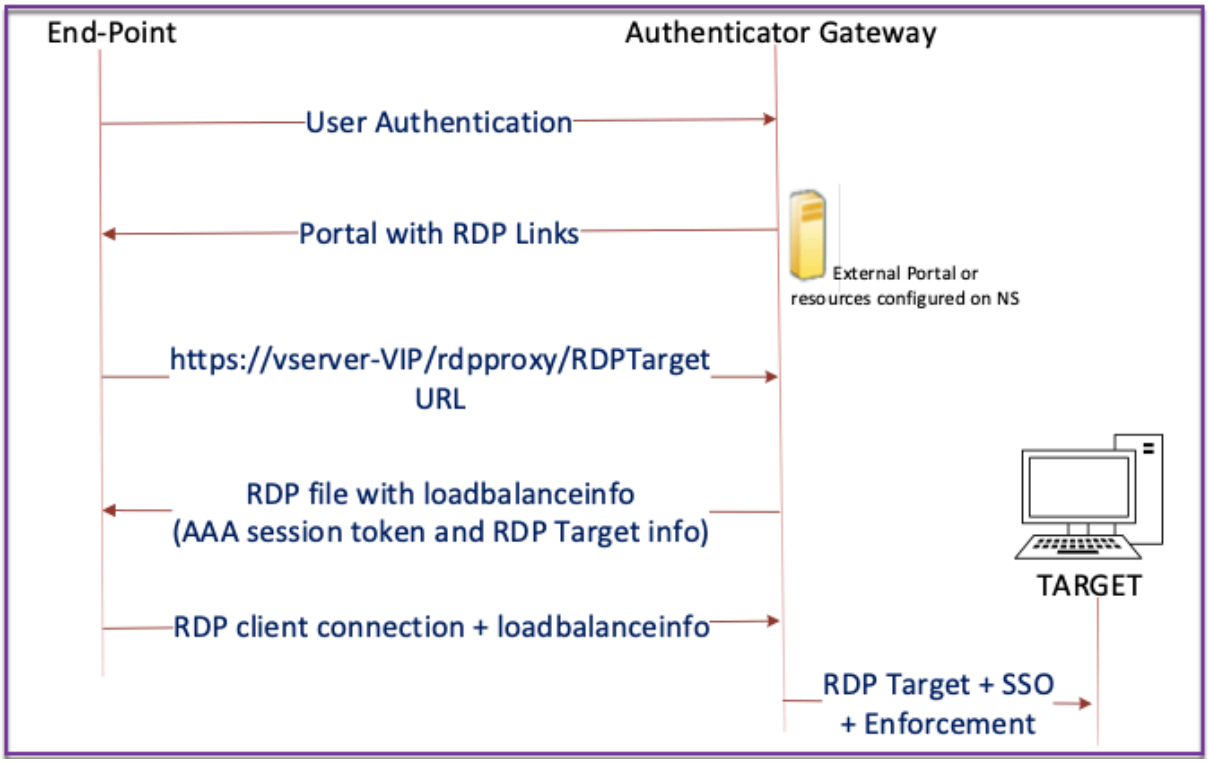
- Una vez que el usuario selecciona un recurso RDP, el VIP de Authenticator Gateway recibe la solicitud en el formato que `https://vserver-vip/rdpproxy/rdptarget/listener` indica el recurso publicado en el que hizo clic el usuario. Esta solicitud contiene la información sobre la dirección IP y el puerto del servidor RDP que el usuario ha seleccionado.
- La puerta de enlace de autenticación procesa la solicitud /rdpproxy/. Dado que el usuario ya está autenticado, esta solicitud incluye una cookie de puerta de enlace válida.
- La información de `RDPTarget` y `RDPUser` se almacena en el servidor STA y se genera un tíquet STA. La información almacenada en el servidor STA se cifra mediante la clave previamente compartida configurada. La puerta de enlace de autenticación utiliza uno de los servidores STA configurados en el servidor virtual de puerta de enlace.
- La información de "Listener"obtenida en la solicitud /rdpproxy/ se coloca `.rdp file` como "`fulladdress`", y el tíquet STA (predefinido con el AuthID de STA) se coloca `.rdp file` como "`loadbalanceinfo`".
- `.rdp file` se devuelve al dispositivo de punto final del cliente.
- El cliente RDP nativo se inicia y se conecta al `RDPListener Gateway`. Envía el tíquet STA en el paquete inicial.

  La puerta de enlace `RDPListener` valida el tíquet de STA y obtiene la información de `RDPTarget` y `RDPUser`. El servidor STA que se va a utilizar se recupera mediante el 'authID' presente en el `loadbalanceinfo`.
- Se crea una sesión de puerta de enlace para almacenar directivas de autorización/auditoría. Si existe una sesión para el usuario, se reutiliza.
- La puerta de enlace `RDPListener` se conecta a `RDPTarget` e inicia sesión con SSO mediante CREDSSP.

> **Importante:**
>
> - Para el proxy RDP sin estado, el servidor STA valida el tíquet STA, enviado por el cliente RDP, para obtener la información de `RDPTarget`/`RDPUser`. Debe enlazar el servidor STA además del servidor virtual VPN.

Compatibilidad con puerta de enlace única

En la siguiente ilustración se muestra la implementación:



> **Importante:**
>
> En el caso de una única implementación de puerta de enlace, el servidor STA no es necesario. La puerta de enlace del autenticador codifica `RDPTarget` y la cookie de sesión de autenticación, autorización y auditoría de NetScaler de forma segura y las envía como `loadbalanceinfo` en el `.rdp file`. Cuando el cliente RDP envía este token en el paquete inicial, la puerta de enlace del autenticador decodifica la información de `RDPTarget`, busca la sesión y se conecta a `RDPTarget`.

Soporte para oyente único

- Escucha única para tráfico RDP y SSL.
- La descarga de archivos RDP y el tráfico RDP se pueden gestionar a través de la misma tupla 2 (es decir, IP y puerto) en el dispositivo NetScaler.

Requisitos de licencia del proxy RDP

Edición premium, modificación avanzada

> **Nota:**
>
> La función RDP Proxy no está disponible para los clientes que solo tienen una licencia de

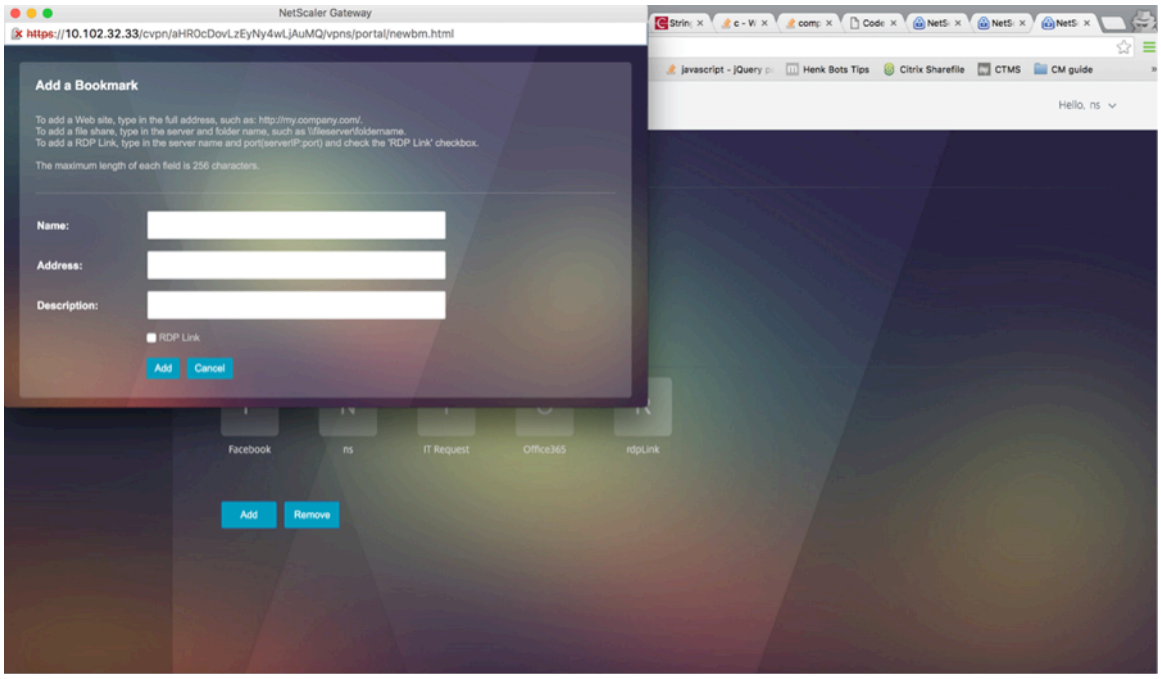
> plataforma Gateway o solo la modificación Standard.

Puede utilizar el siguiente comando para habilitar el proxy RDP.

```
enable feature rdpProxy
<!--NeedCopy-->
```

Marcador

Generación de enlaces RDP mediante Portal. En lugar de configurar los vínculos RDP para el usuario o publicar los vínculos RDP a través de un portal externo, puede dar a los usuarios la opción de generar sus propias URL proporcionando `targerIP:Port`. Para la implementación de proxy RDP sin estado, el administrador puede incluir información del listener RDP en FQDN: Formato de puerto como parte del perfil de cliente RDP. Esto se hace bajo la opción `rdpListener`. Esta configuración se utiliza para la generación de enlaces RDP a través del portal en modo de puerta de enlace dual.



Crear marcadores

1. Cree marcadores en la página del portal para acceder a los recursos de RDP: (ActualURL comienza por `rdp://`).
2. Agregar url de VPN `<urlName> <linkName> <actualURL>`
    - La dirección URL debe tener el siguiente formato: `rdp://<TargetIP:Port>`.

- Para el modo proxy RDP sin estado, la URL debe tener el siguiente formato: `rdp://<TargetIP:Port>/<ListenerIP:Port>`
- La URL se publica en el portal en el formato:
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>`
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. Enlaza los marcadores al usuario, grupo, servidor virtual VPN o VPN global.

Funciones y modos que se habilitan para el proxy RDP

```
-  enable ns feature ssl

-  enable ns feature sslvpn

-  enable ns feature rdpproxy

-  enable mode usnip
<!--NeedCopy-->
```

Pasos de configuración de alto nivel para el proxy

Los siguientes pasos de alto nivel implicados en la configuración del proxy RDP sin estado.

- Crear un perfil de servidor RDP
- Creación de un perfil de cliente RDP
- Crear y enlazar un servidor virtual
- Crear un marcador
- Crear o modificar un perfil o una directiva de sesión
- Enlazar un marcador

Configurar un perfil de cliente

Configure el perfil del cliente en la puerta de enlace del autenticador. A continuación se muestra un ejemplo de configuración:

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as ‘ fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
```



```
      redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
       | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
<!--NeedCopy-->
```

Asocie el perfil del cliente RDP al servidor virtual VPN.

Esto se puede hacer configurando una SessionAction+sessionPolicy o estableciendo el parámetro VPN global.

Ejemplo:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
   prioritynumber>
<!--NeedCopy-->
```

O BIEN:

```
set vpn parameter  – rdpClientprofile <name>
<!--NeedCopy-->
```

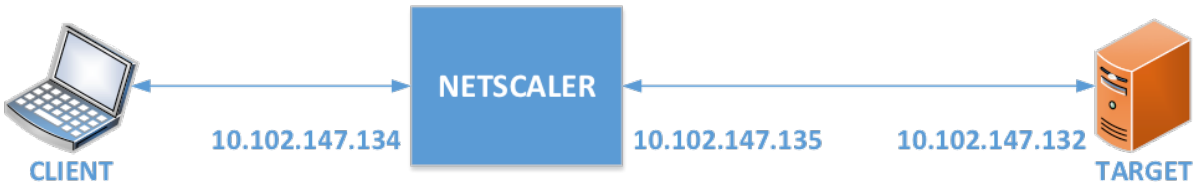
Configurar un perfil de servidor

Configure el perfil del servidor en la puerta de enlace del listener.

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
   listener> -rdpPort <port for terminating RDP client connections> -
   psk <key to decrypt RDPTarget/RDPUser information, needed while
   using STA>`
<!--NeedCopy-->
```

`rdp ServerProfile` debe configurarse en el servidor virtual VPN.

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
   rdpServerProfile <rdpServer Profile>`
<!--NeedCopy-->
```



Configuración del proxy RDP mediante la CLI

A continuación se muestra un ejemplo de configuración del proxy RDP mediante la CLI.

- Agregue la URL de VPN del usuario con la información de destino.

```
add aaa user Administrator  –password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator   –urlName rdp
<!--NeedCopy-->
```

- Configure el perfil de cliente y servidor RDP para la conexión VPN.

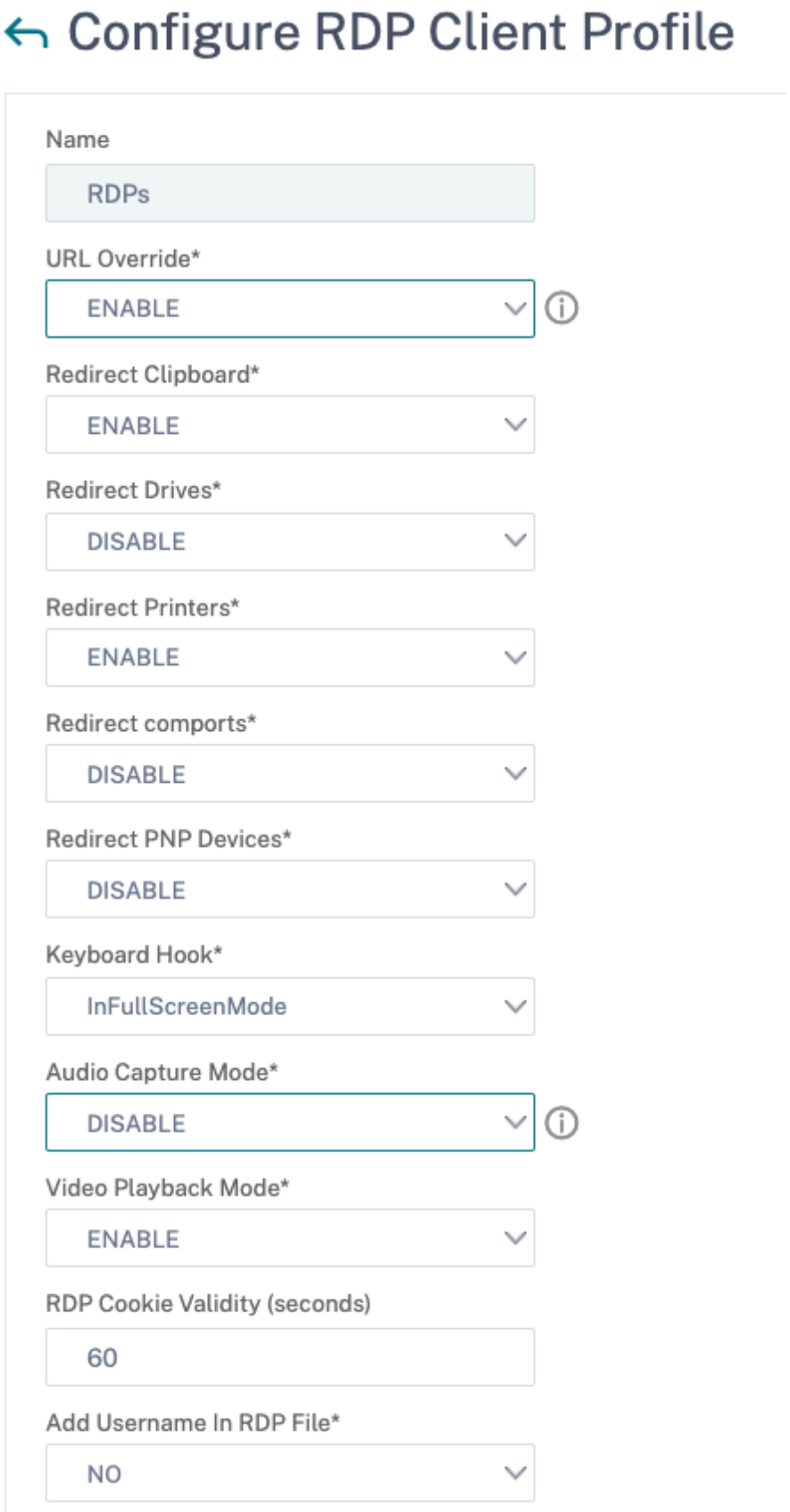
```
add rdp clientprofile p1  –psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443  –
   rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
   defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
   rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

- AGREGAR SNIP para la conexión de NetScaler al destino.

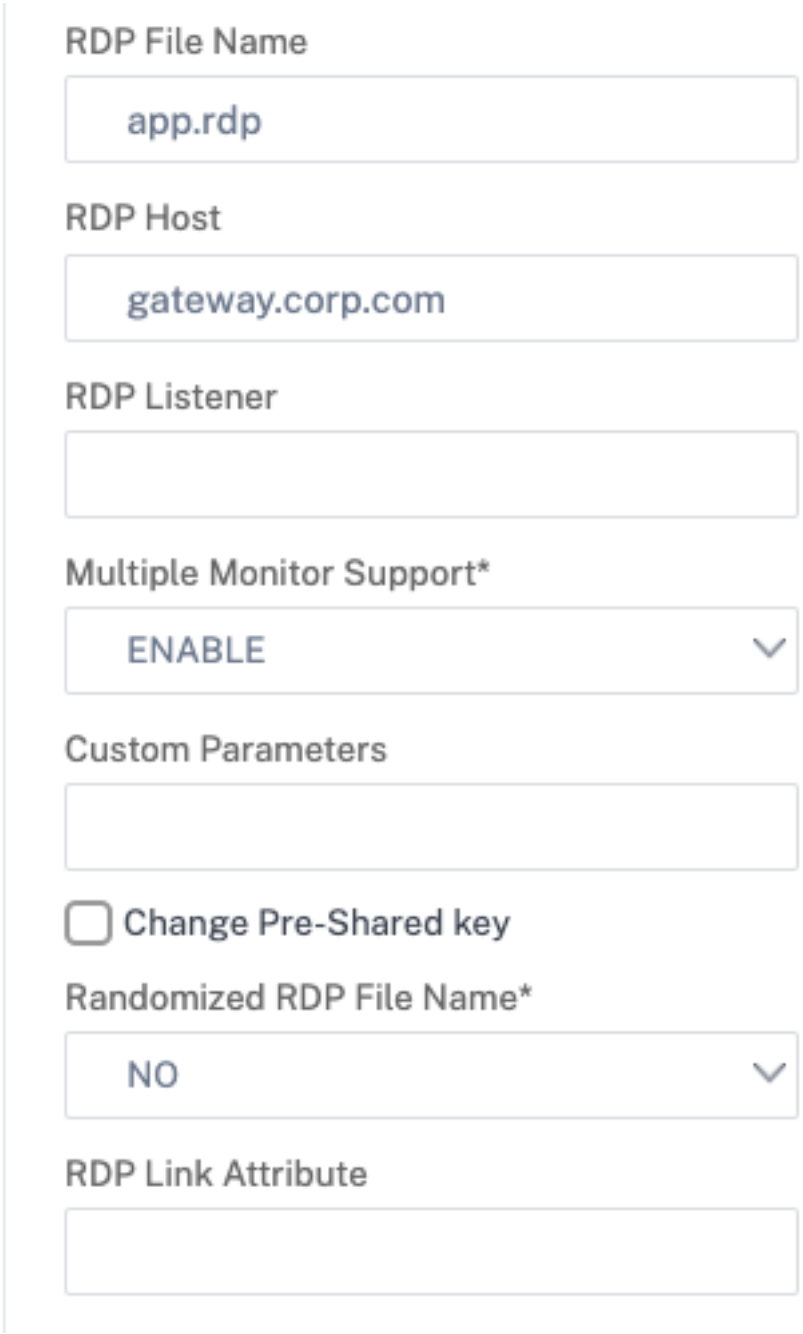
```
add ns ip 10.102.147.135  255.255.255.0  –type SNIP
<!--NeedCopy-->
```

Configuración del proxy RDP mediante la interfaz gráfica de usuario

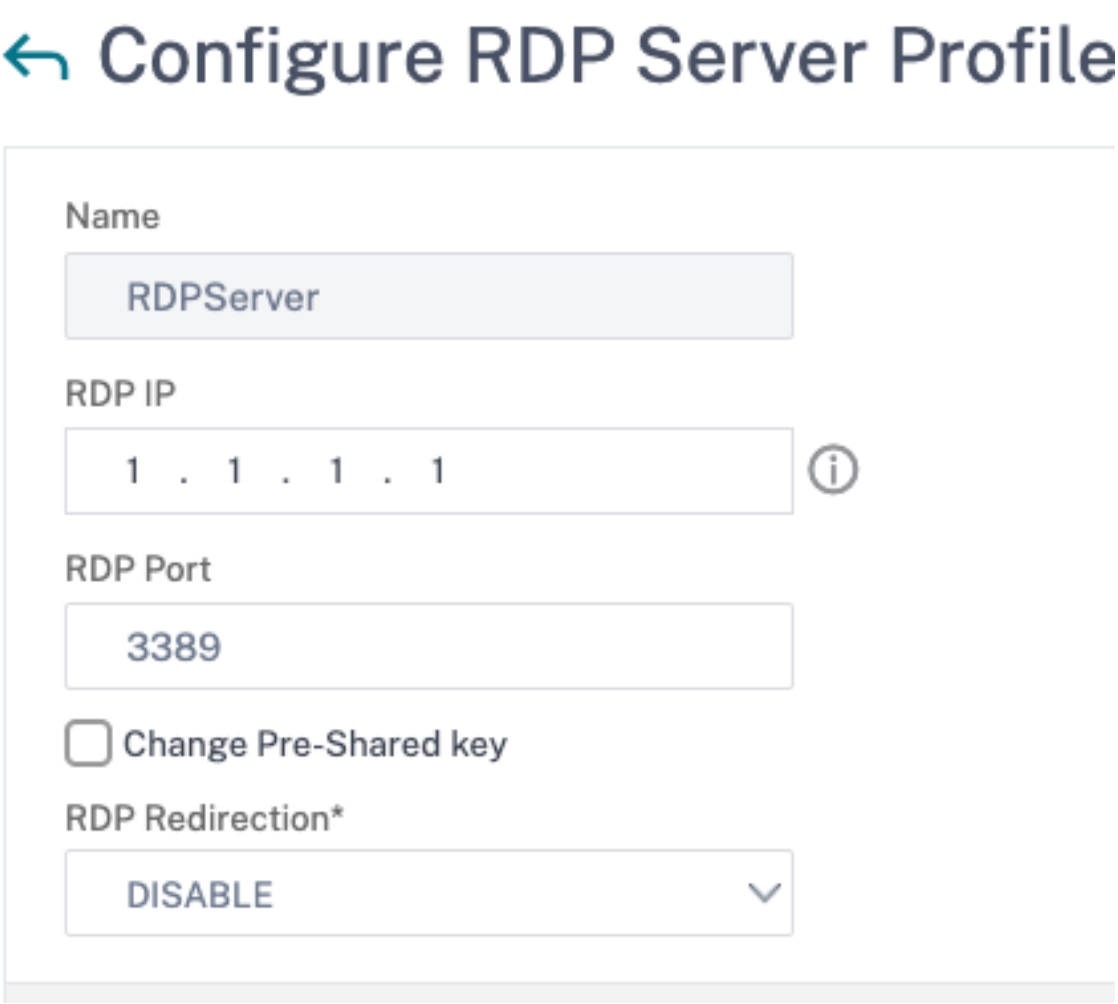
1. Vaya a **NetScaler Gateway > Directivas**, haga clic con el botón derecho en **RDP**y haga clic en **Activar función**
2. Haga clic en RDP en el panel de navegación. A la derecha, selecciona la ficha **Perfiles de cliente** y haga clic en **Agregar**.
3. Introduzca un nombre para el perfil del cliente y configúrelo.



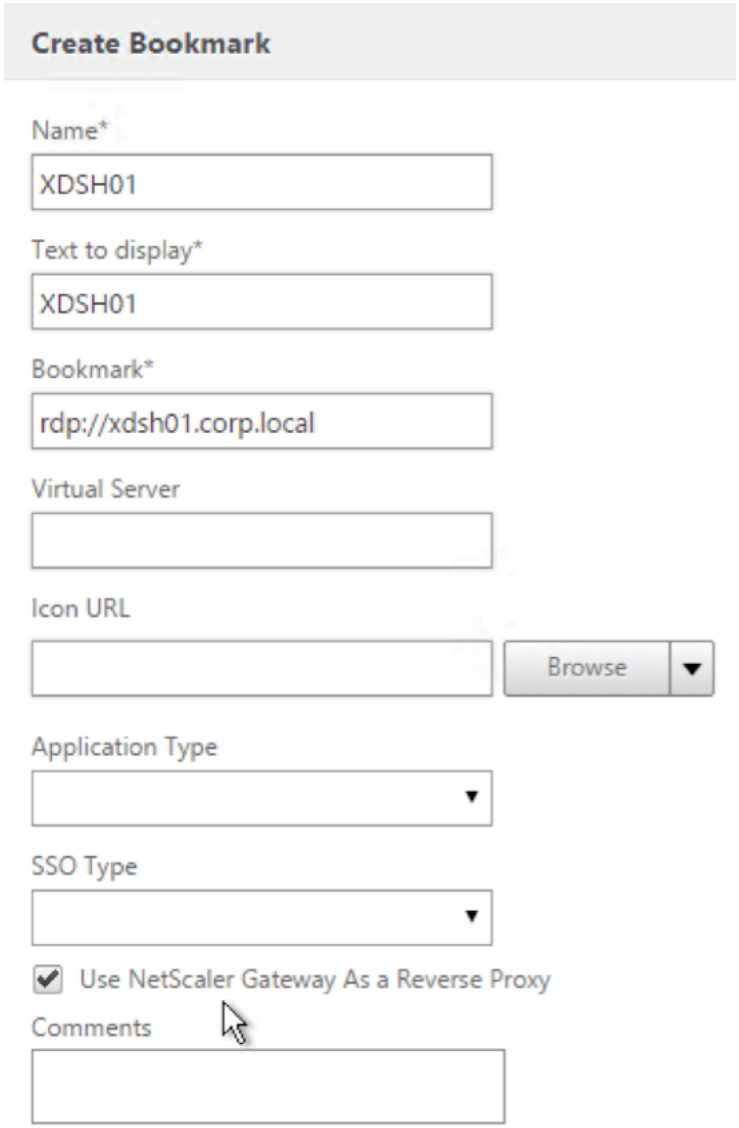
4. En el campo Host de RDP, introduzca el FQDN que se resuelve en la escucha del proxy RDP, que suele ser el mismo FQDN que el FQDN del dispositivo NetScaler Gateway.
5. En **Clave previamente compartida**, introduzca una contraseña y haga clic en **Aceptar**.



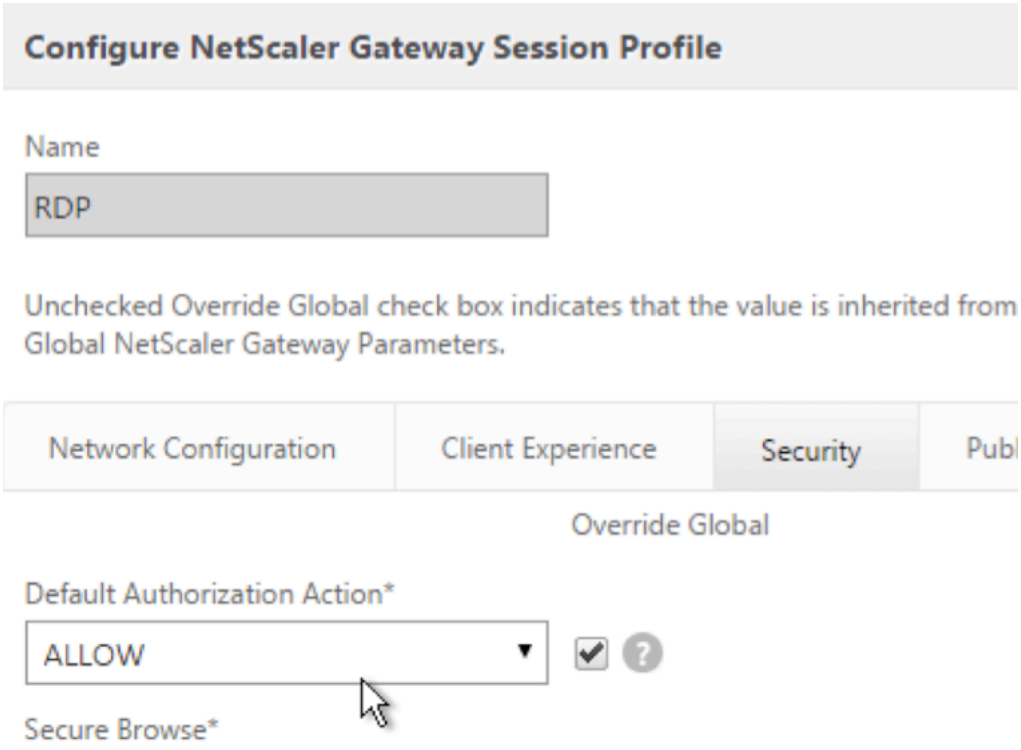
6. Introduzca un nombre en el perfil del servidor.
7. Introduzca la dirección IP del servidor virtual de puerta de enlace al que va a enlazar este perfil.
8. Introduzca la misma clave previamente compartida que configuró para el perfil de cliente RDP. Haga clic en **Crear**.



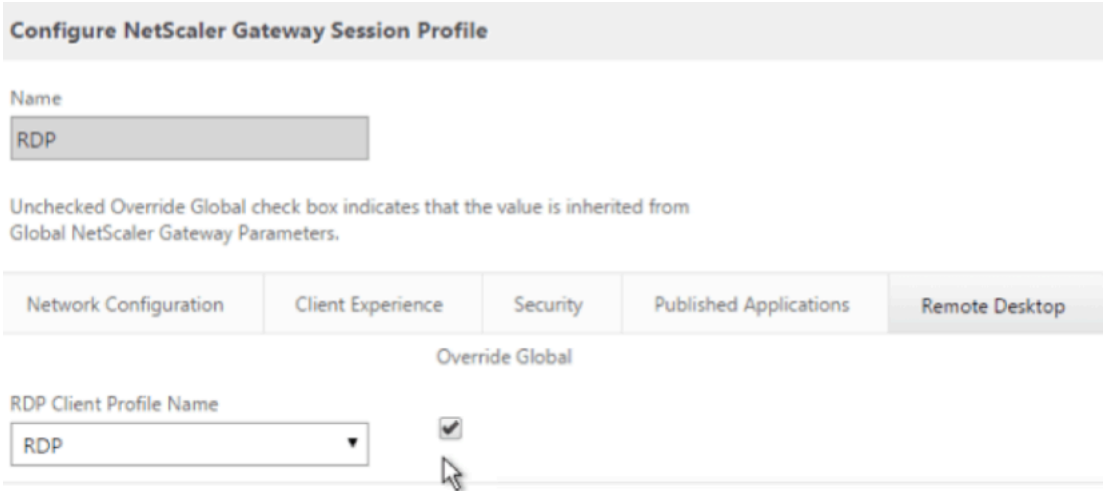
9. Si quiere agregar marcadores de RDP en la página del portal de acceso sin cliente, a la izquierda, expanda **NetScaler Gateway**, expanda **Recursos**y haga clic en **Marcadores**.
10. A la derecha, haga clic en **Agregar**.
11. Ponle un nombre al marcador.
12. Para la URL, escriba **rdp: //myRDPServer mediante IP o DNS**.
13. Seleccione Usar **NetScaler Gateway como proxy inverso** y haga clic en **Crear**.
14. Cree marcadores según sus necesidades.



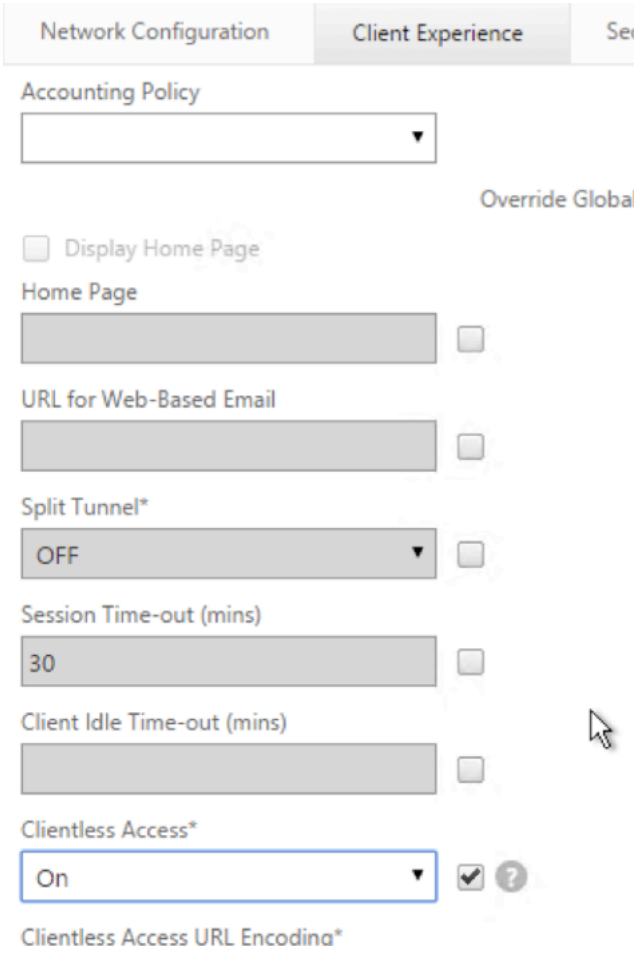
15. Crea o modifica un perfil de sesión. Vaya a **NetScaler Gateway > Directivas > Sesión**.
16. En la ficha Seguridad, establezca **Acción de autorización predeterminada** en **Permitir**. O bien, puede utilizar directivas de autorización para controlar el acceso.



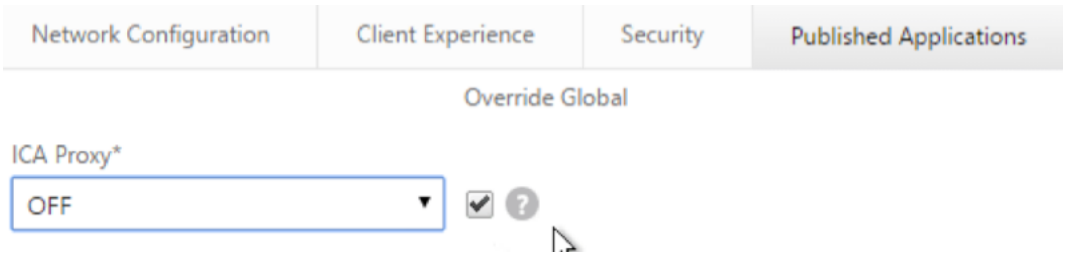
17. En la ficha Escritorio remoto, seleccione el perfil de cliente RDP que creó anteriormente.



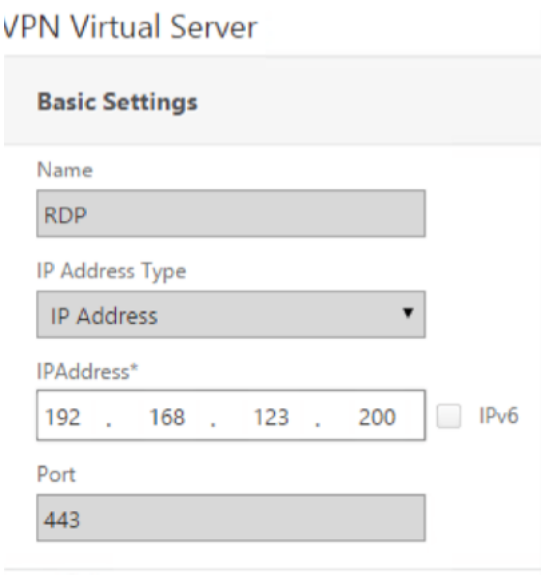
18. Si quiere utilizar marcadores, en la ficha **Experiencia del cliente**, establezca **Acceso sin clienteen On**.



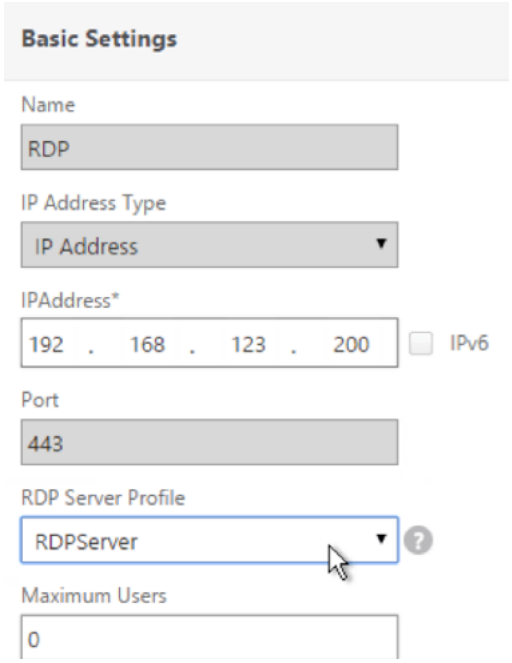
19. En la ficha **Aplicaciones publicadas**, asegúrese de que el proxy ICA esté **DESACTIVADO**.



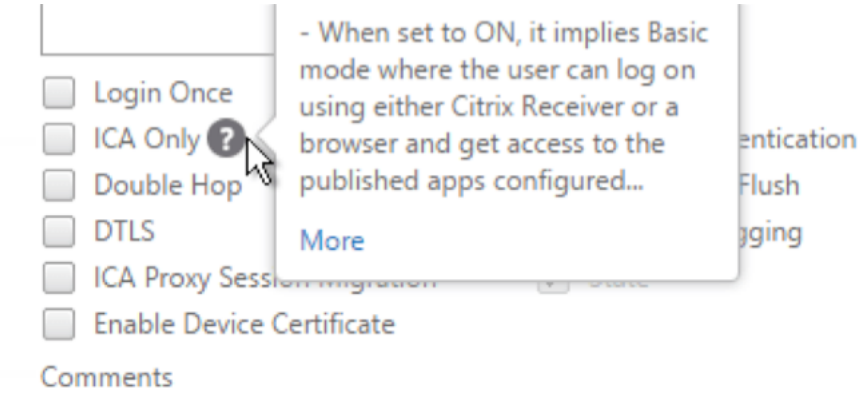
20. Modifique o cree su servidor virtual de puerta de enlace.
21. En la sección **Configuración básica**, haga clic en **Más**.



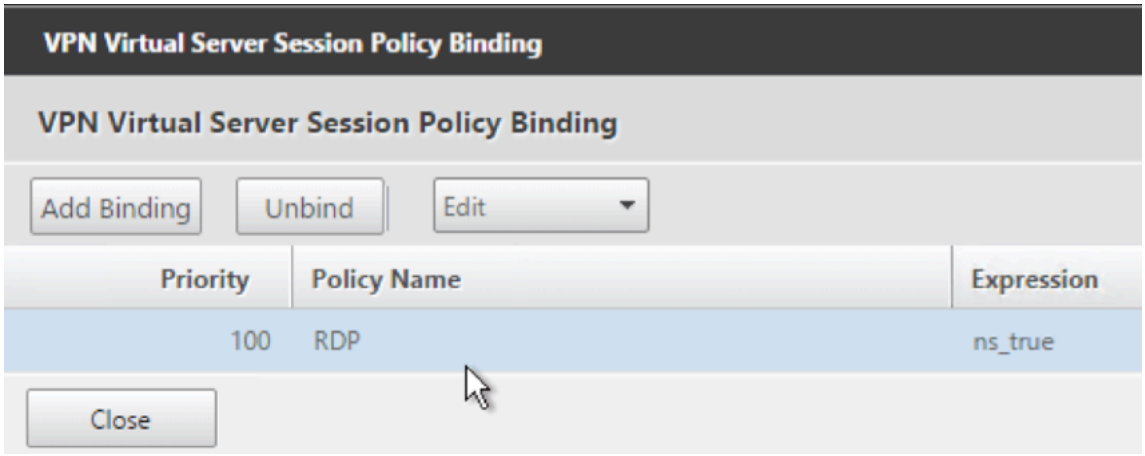
22. Utilice la lista de perfiles de servidor RDP para seleccionar el perfil de servidor RDP que creó anteriormente.



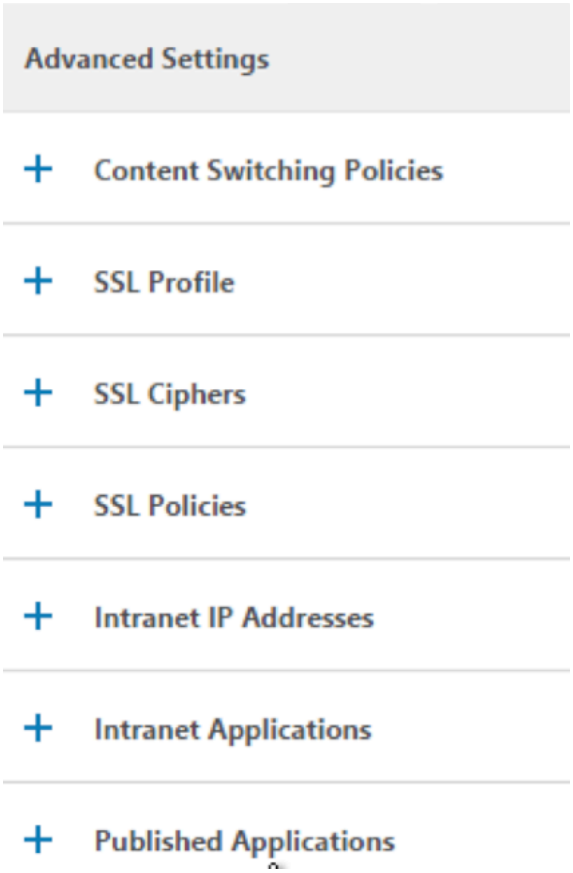
23. Desplácese hacia abajo. Asegúrese de que **solo ICA** no esté marcada.



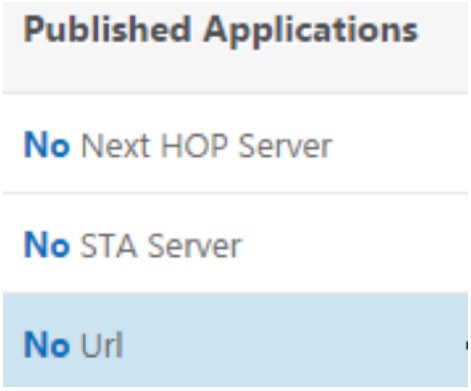
24. Enlazar un certificado.
25. Enlazar directivas de autenticación.
26. Enlazar la directiva/perfil de sesión que tiene configurado el perfil de cliente RDP.



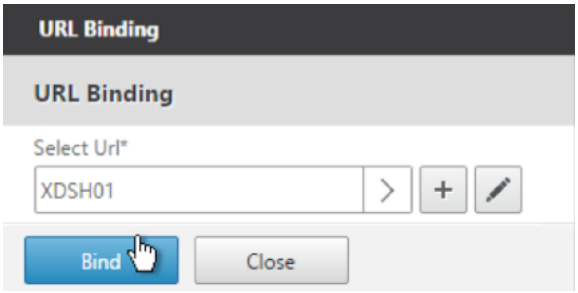
27. Puede enlazar marcadores al servidor virtual de NetScaler Gateway o a un grupo de autenticación, autorización y auditoría. Para enlazar con el servidor virtual de NetScaler Gateway, a la derecha, en la sección Configuración avanzada, haga clic en **Aplicaciones publicadas**.



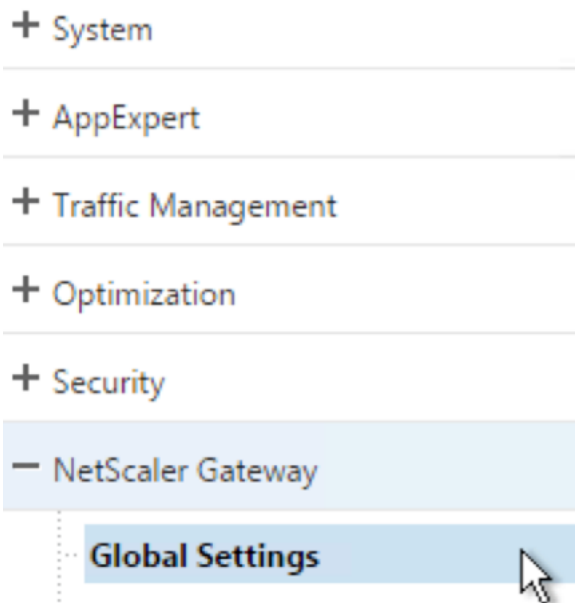
28. A la izquierda, en la sección **Aplicaciones publicadas**, haga clic en **Sin URL**.



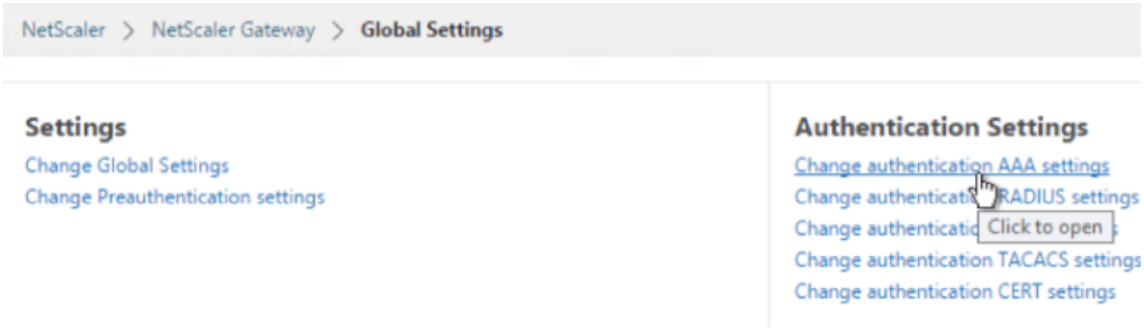
29. Enlace sus marcadores.



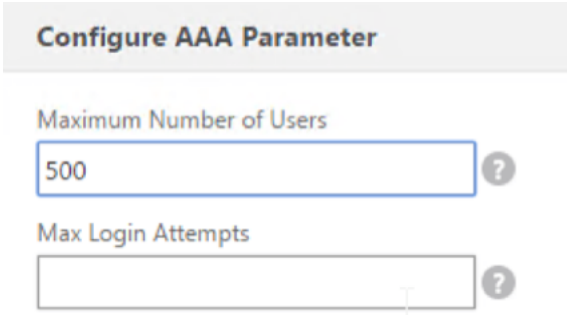
30. Dado que solo ICA no se especifica para este servidor virtual de NetScaler Gateway, asegúrese de que las licencias universales de NetScaler Gateway estén configuradas correctamente. A la izquierda, expanda **NetScaler Gateway** y haga clic en **Configuración global**.



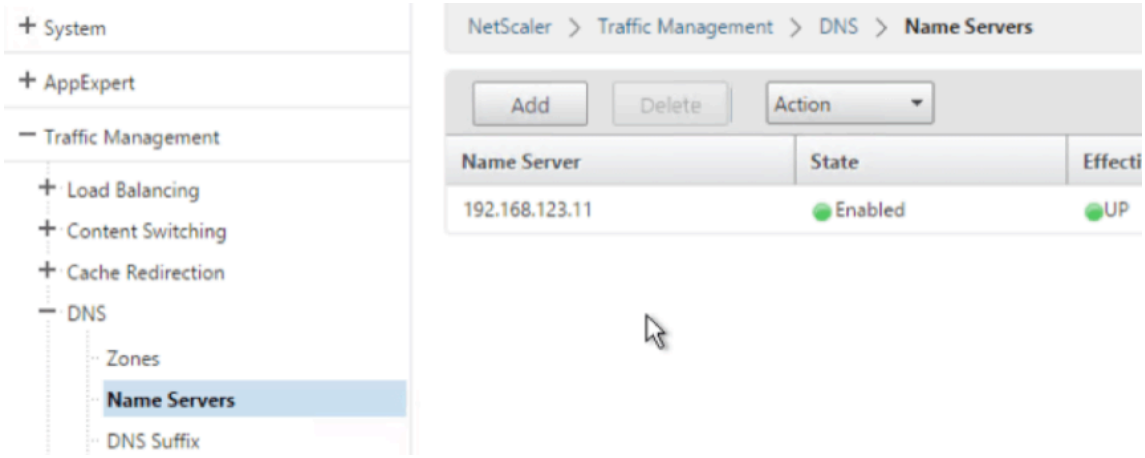
31. A la derecha, haga clic en **Cambiar configuración de autenticación AAA**.



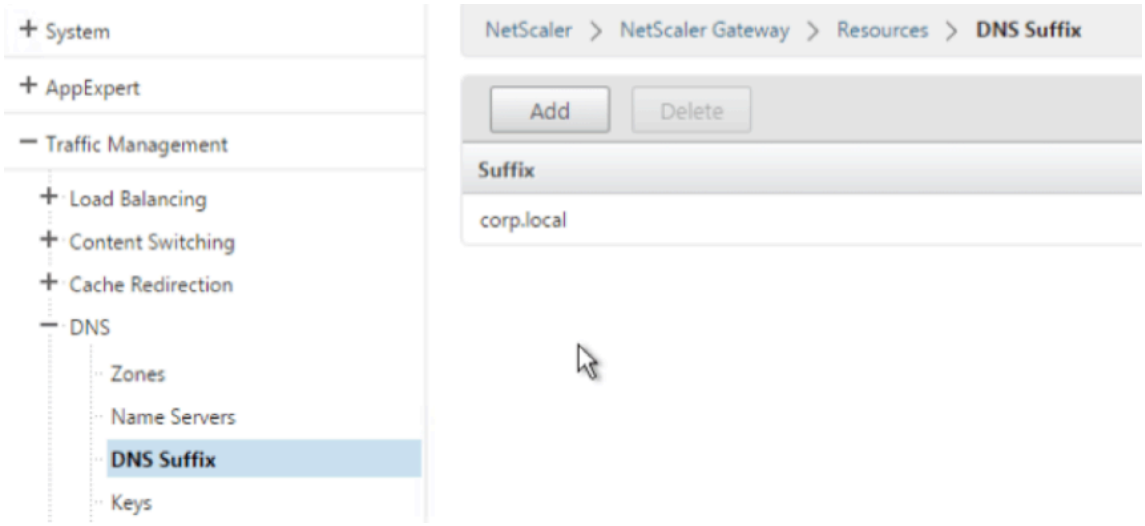
32. Cambie el **número máximo de usuarios** al límite con licencia.



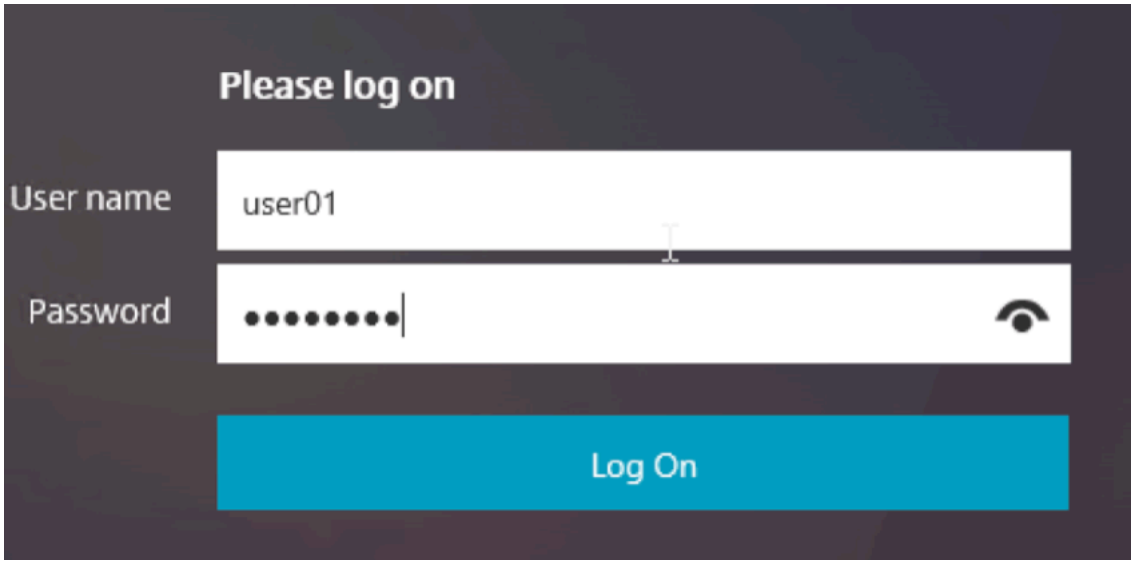
33. Si quiere conectarse a servidores RDP mediante DNS, asegúrese de que los servidores DNS estén configurados en el dispositivo (**Administración del tráfico > DNS > Servidores de nombres)**.



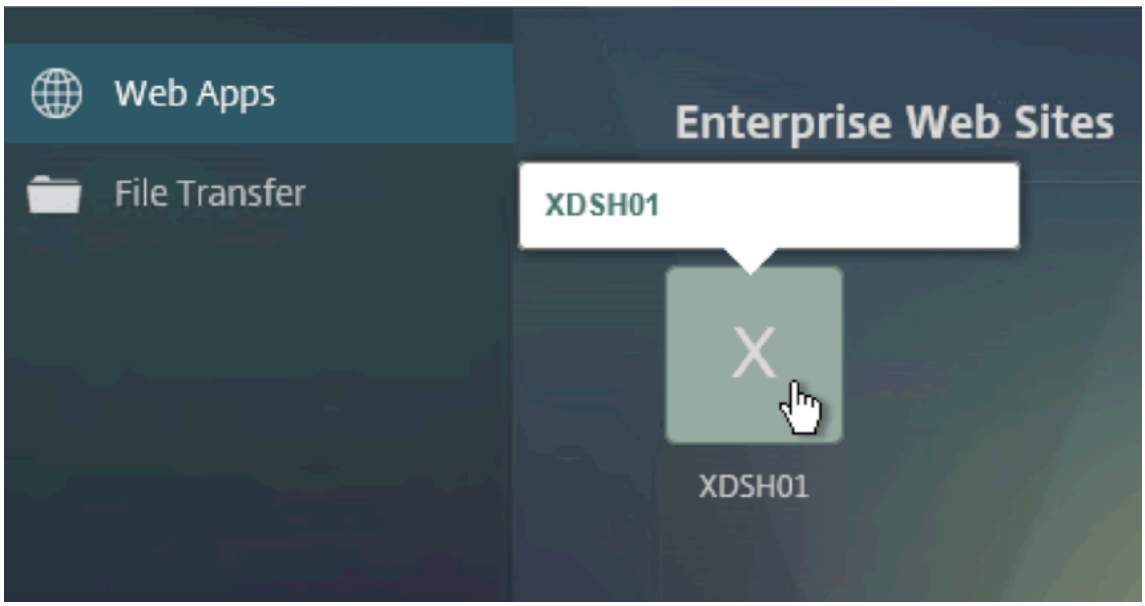
34. Si quiere utilizar los nombres cortos en lugar de los FQDN, agregue un **sufijo DNS (Administración del tráfico > DNS > Sufijo DNS)**.



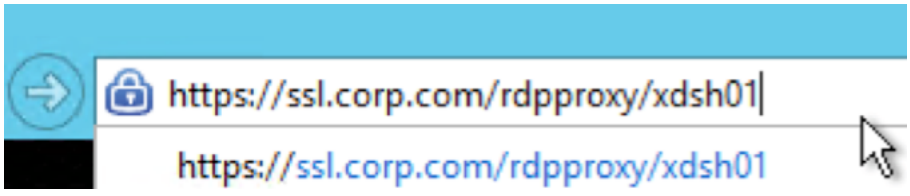
35. Conéctate a su puerta de enlace e inicia sesión.



36. Si ha configurado **Marcadores**, haga clic en el **marcador**.

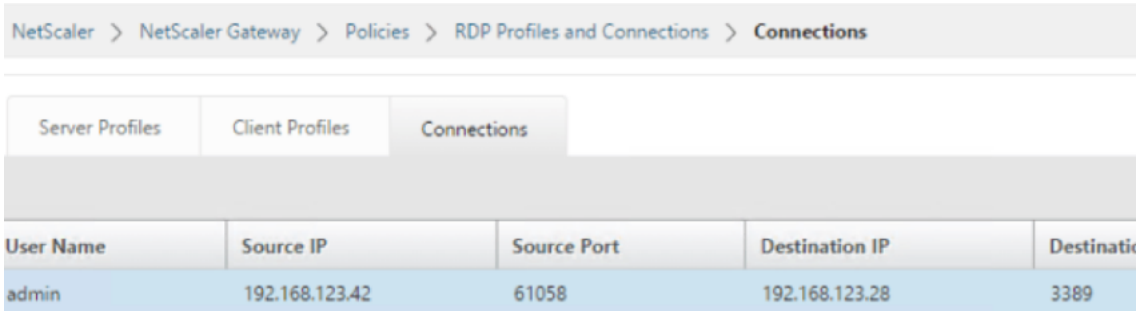


37. Puede cambiar la barra de direcciones a **/rdpProxy/myrdpServer**. Puede introducir una dirección IP (por ejemplo rdpproxy/192.168.1.50) o un nombre DNS (/rdpproxy/myserver).



38. Abre el archivo descargado `.rdp file`.

39. Para ver los usuarios conectados actualmente, vaya a **NetScaler Gateway Policies > RDP.** A la derecha está la ficha **Conexiones**.



Opción para inhabilitar el SSO

La función SSO (inicio de sesión único) con proxy RDP se puede inhabilitar mediante la configuración de directivas de tráfico de NetScaler para que siempre se pidan credenciales al usuario. Cuando el SSO está inhabilitado, la aplicación de RDP (SmartAccess) no funciona.

Ejemplo:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
<!--NeedCopy-->
```

La directiva de tráfico se puede configurar según el requisito; a continuación se muestran dos ejemplos:

- Para inhabilitar el inicio de usuario único para todo el tráfico:

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy
   " <TrafficActionName>
<!--NeedCopy-->
```

- Para inhabilitar SSO basado en IP/FQDN de origen/destino

```
add vpn trafficPolicy <TrafficPolicyName>  "HTTP.REQ.URL.CONTAINS
   ("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
<!--NeedCopy-->
```

Proxy RDP sin estado

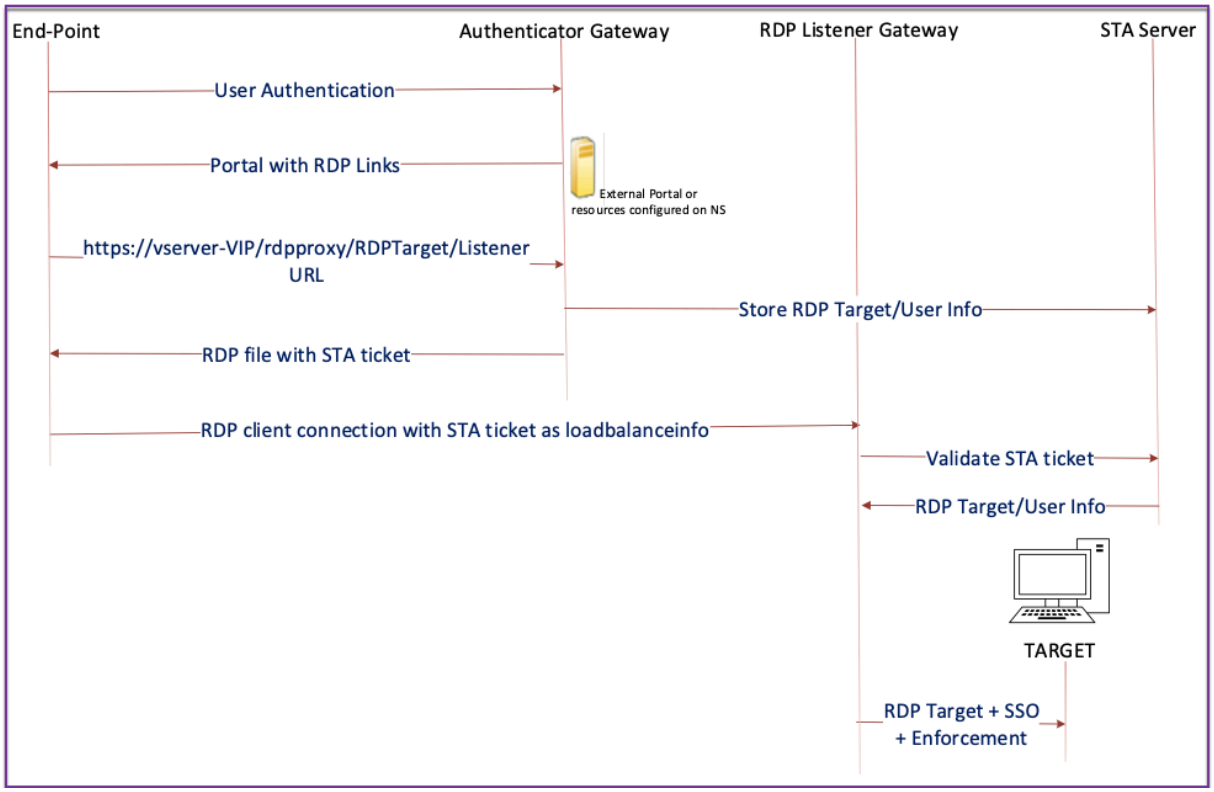
January 26, 2024

El proxy RDP sin estado accede a un host RDP. El acceso se concede a través de `RDPListener` en NetScaler Gateway cuando el usuario se autentica en un NetScaler Gateway Authenticator independiente. La información requerida `RDPListener` por NetScaler Gateway se almacena de forma segura en un servidor STA. Un servidor STA se puede colocar en cualquier lugar siempre que NetScaler Gateway y los servidores de enumeración de aplicaciones puedan llegar a él. Para obtener más información, consulte https://support.citrix.com/article/CTX101997.

Flujo de conexión

Hay dos conexiones involucradas en el flujo del proxy RDP. La primera conexión es la conexión VPN SSL del usuario con el VIP de NetScaler Gateway y la enumeración de los recursos RDP.

La segunda conexión es la conexión del cliente RDP nativo con el listener RDP (configurado mediante RDPIP y RDPport) en NetScaler Gateway, y la subsiguiente transmisión del cliente RDP a los paquetes del servidor de forma segura.



1. El usuario se conecta a la VIP de puerta de enlace de autenticación y proporciona las credenciales.
2. Tras iniciar sesión correctamente en la puerta de enlace, se redirige al usuario a la página de inicio/portal externo, que enumera los recursos de escritorio remoto a los que puede acceder el usuario.

3. Una vez que el usuario selecciona un recurso RDP, el VIP de Authenticator Gateway recibe una solicitud en el formato que `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` indica el recurso publicado en el que el usuario ha hecho clic. Esta solicitud contiene la información sobre la IP y el puerto del servidor RDP que el usuario ha seleccionado.
4. La puerta de enlace del autenticador procesa la solicitud /rdpproxy/. Dado que el usuario ya está autenticado, esta solicitud incluye una cookie de puerta de enlace válida.
5. La información de `RDPTarget` y `RDPUser` se almacena en el servidor STA y se genera un tíquet STA. La información se almacena como un blob XML que se cifra opcionalmente mediante la clave previamente compartida configurada. Si se cifra, el blob se codifica y almacena en base64. La puerta de enlace de autenticación utiliza uno de los servidores STA configurados en el servidor virtual de puerta de enlace.
6. El blob XML tiene el siguiente formato

```
<Value name=”IPAddress”>ipaddr</Value>\n<Value name=”Port”>
    port</Value>n

<Value name=”`Username`”>username</Value>\n<Value name=”
    Password”>pwd</Value>
<!--NeedCopy-->
```

7. El `rdptargetproxy` obtenido en la solicitud /rdpproxy/ se coloca como “`fulladdress`” y el tíquet STA (predefinido con el AuthID de STA) se coloca como `loadbalanceinfo` en el archivo RDP.
8. El archivo `.rdp` se devuelve al punto final del cliente.
9. El cliente RDP nativo se inicia y se conecta al `RDPListener Gateway`. Envía el tíquet STA en el paquete x.224 inicial.
10. `RDPListener Gateway` valida el tíquet STA y obtiene la información de `RDPTarget` y `RDPUser`. El servidor STA que se va a utilizar se recupera mediante el ‘authID’presente en el `loadbalanceinfo`.
11. Se crea una sesión de puerta de enlace para almacenar directivas de autorización/auditoría. Si existe una sesión para el usuario, se reutiliza.
12. `RDPListener Gateway` se conecta a `RDPTarget` e inicia sesión con SSO mediante CREDSSP.

Requisitos previos

- El usuario se autentica en el autenticador de NetScaler Gateway.
- La URL /rdpproxy inicial y el cliente RDP están conectados a otro `RDPListener NetScaler Gateway`.

- La puerta de enlace de autenticación que utiliza un servidor STA transmite la información de `RDPListener Gateway` de forma segura.

Configurar proxy RDP sin estado mediante la CLI

- Agrega un perfil `rdpServer`. El perfil del servidor está configurado en `RDPListener Gateway`.

  Nota:

  - Una vez configurado el perfil de RDPServer en el servidor virtual VPN, no se puede modificar. Además, el mismo ServerProfile no se puede reutilizar en otro servidor virtual VPN.

```
add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
   RDP listener] -rdpPort [port for terminating RDP client
   connections] -psk [key to decrypt RDPTarget/RDPUser
   information, needed while using STA].
<!--NeedCopy-->
```

  Configure el perfil del servidor RDP en el servidor virtual VPN mediante el siguiente comando:

```
add vpn vserver v1 SSL [publicIP] [
   portforterminatingvpnconnections] -rdpServerProfile [rdpServer
    Profile]
<!--NeedCopy-->
```

  Ejemplo

```
add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile
   rdp_server_prof
<!--NeedCopy-->
```

  Importante:

  - El mismo servidor STA debe estar enlazado tanto a la puerta de enlace de autenticación RDP como a la puerta de enlace de escucha.
  - En el caso del proxy RDP sin estado, el servidor STA valida el ticket STA que envía el cliente RDP para obtener la información del servidor de destino de RDP y del usuario de RDP. Debe enlazar el servidor STA además del servidor virtual VPN. En el siguiente ejemplo, el servidor de destino RDP es 1.1.1.0 y el servidor virtual RDP listener Gateway 1.1.1.2.

```
      add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
<!--NeedCopy-->
```

Configure el perfil del cliente en la puerta de enlace del autenticador mediante el siguiente comando:


```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put
    in the RDP file as ‘fulladdress’> [-rdpUrlOverride ( ENABLE |
    DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-
    redirectDrives ( ENABLE | DISABLE )]

        [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <
            keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
            videoPlaybackMode ( ENABLE | DISABLE )]

        [-rdpCookieValidity <positive_integer>][-multiMonitorSupport (
            ENABLE | DISABLE )] [-rdpCustomParams <string>]
<!--NeedCopy-->
```

La configuración —RDPhost se utiliza en una única implementación de puerta de enlace. Solo `psk` es un argumento obligatorio y debe ser el mismo PSK que se agrega al perfil del servidor RDP en la puerta de enlace de escucha de RDP.

- Asocie el perfil RDP al servidor virtual VPN.

Puede asociar un perfil RDP configurando una SessionAction+SessionPolicy o estableciendo el parámetro VPN global.

Ejemplo:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
<!--NeedCopy-->
```

O BIEN:

```
set vpn parameter  – rdpClientprofile <name>
<!--NeedCopy-->
```

Configurar el proxy RDP sin estado mediante la interfaz gráfica de usuario

Los siguientes pasos de alto nivel están implicados en la configuración del proxy RDP sin estado. Para ver los pasos detallados, consulte Configuración del proxy RDP.

- Crear un perfil de servidor RDP
- Creación de un perfil de cliente RDP
- Crear un servidor virtual
- Crear un marcador
- Crear o modificar un perfil o una directiva de sesión

- Enlazar un marcador

> **Importante:**
>
> Para el proxy RDP sin estado, debe enlazar un servidor STA además del servidor virtual VPN.

Contador de conexiones

Se ha agregado un nuevo contador de conexiones ns_rdp_tot_curr_active_conn, que mantiene el registro del número de conexiones activas en uso. Se puede ver como parte del comando `nsconmsg` en el shell de NetScaler. El comando CLI para ver estos contadores está previsto que se agregue más adelante.

Notas de la actualización

El RDPIP y el RDPport, que se configuraron previamente en el servidor virtual VPN, forman parte del RDPServerProfile. `rdp Profile` cambia de nombre a `rdp ClientProfile` y se elimina el parámetro clientSSL. Por lo tanto, la configuración anterior no funciona.

Redirección de conexiones RDP

January 26, 2024

Un dispositivo NetScaler Gateway admite ahora la redirección de conexiones RDP en presencia de un agente de conexiones o un directorio de sesiones. Una comunicación proxy RDP ya no requiere una URL exclusiva para cada conexión del cliente al servidor. En su lugar, el proxy utiliza una única URL para conectarse a una comunidad de servidores RDP, lo que reduce la sobrecarga de mantenimiento y configuración de un administrador.

Punto a tener en cuenta:

- La redirección de conexiones RDP solo se admite cuando el SSO está habilitado y se admite tanto en modo de puerta de enlace única como en modo de puerta de enlace sin estado o puerta de enlace doble junto con la aplicación (SmartAccess).
- La función RDP Proxy solo es compatible con la redirección basada en tokens que admite cookies IP. Los tokens de redirección basados en IP “msts=”los devuelve el agente de sesiones de Windows o el agente de conexión cuando la funcionalidad **Usar redirección de direcciones IP** está inhabilitada.

- Puede inhabilitar la opción **Usar redirección de direcciones IP** para habilitar la redirección basada en tokens en la siguiente ubicación.
  `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker`.
- Inhabilite la opción Usar redirección de direcciones IP en los equipos RDSH y no en el equipo del agente de conexiones.
- Se pueden configurar redireccionadores dedicados para la conexión de proxy RDP.

Requisitos previos

- Cree un perfil de servidor RDP para habilitar el agente de escucha 3389 en el servidor virtual de NetScaler Gateway.
  Si la máquina que quiere RDP no es miembro de ninguna infraestructura de agente de conexiones de RDS, no necesita el agente de escucha 3389.
- Habilite la redirección de conexiones RDP en el dispositivo NetScaler Gateway para admitir el proxy RDP en presencia de un agente de conexiones.

Implementar proxy RDP en presencia de un agente de conexión

El proxy RDP en presencia de un agente de conexión se puede implementar de las dos formas siguientes.

- Con servidores host de sesión de Escritorio remoto que participan en el equilibrio de carga del agente de conexiones de Escritorio remoto.
- En presencia de la función de equilibrio de carga de RDP.

Con servidores host de sesión de Escritorio remoto que participan en el equilibrio de carga del agente de conexiones de Escritorioremoto:

En este caso, el enlace URL de RDP se puede configurar para que apunte a uno de los servidores RDP como servidor de destino, que actúa como redirector. Además, es posible tener uno de los servidores RDP de la comunidad como servidor de destino (en este caso, el servidor no acepta ninguna sesión RDP).

En presencia de la función de equilibrio de carga RDP:

Cuando el equilibrio de carga del agente de conexión no está habilitado, podemos tener la función de equilibrio de carga de RDP disponible en NetScaler para realizar el equilibrio de carga necesario de las sesiones de RDP en presencia de un agente de conexión. En este caso, el enlace URL de RDP debe configurarse para que el equilibrador de cargas RDP sea el servidor de destino. El equilibrador

de carga RDP puede estar en el mismo dispositivo NetScaler Gateway que el proxy RDP. Para obtener más información, consulte Servidores RDP de equilibrio de carga.

Configurar el proxy RDP en presencia de un agente de conexión mediante la CLI

En la línea de comandos, escriba;

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
    DISABLE )

add rdpserverprofile serverProfileName -psk " secretString " -
    rdpRedirection ENABLE
<!--NeedCopy-->
```

Configurar la redirección de conexiones RDP mediante la GUI de NetScaler

1. Vaya a **NetScaler Gateway > Políticas > RDP** .
2. Haga clic con el botón derecho en **RDP** para **habilitaro inhabilitar** la funcionalidad de redirección RDP.

Rellenar URL de RDP según el atributo LDAP

January 26, 2024

Puede configurar un dispositivo NetScaler Gateway para recuperar una lista de servidores RDP (IP/FQDN) de un atributo de servidor LDAP. Según la lista recuperada, el dispositivo muestra las URL de RDP de los servidores a los que puede acceder un usuario.

Para rellenar las URL de RDP según el atributo LDAP mediante la CLI

En la línea de comandos, escriba:

```
add rdpclientprofile <Name>  – rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName  – rdpUrlLinkAttribute
    rdpServerAttribute

<!--NeedCopy-->
```

En el ejemplo anterior, RDPServerAttribute corresponde a los detalles del servidor RDP de un usuario determinado del servidor LDAP.

Nota: Para obtener los detalles del atributo LDAP del servidor LDAP, la acción LDAP debe configurarse con la misma cadena que se configura `pUrlLinkAttribute` como se indica a continuación.

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
    <"domain name"> -ldapBindDn <username> -ldapLoginName
   sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
   ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
   ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

Configuración del servidor LDAP

En el servidor LDAP, lleve a cabo los siguientes pasos:

1. Vaya a un **usuario**concreto.
2. En **Usuarios y equipos de AD**, haga clic en **Ver** y, a continuación, en **Detalles**.
3. Haga clic con el botón derecho del ratón en el **nombre de usuarioy,**
4. Cambie el valor del atributo requerido (displayName) y haga clic en **Aceptar.**

Para rellenar las URL de RDP basadas en el atributo LDAP mediante la interfaz gráfica de usuario

1. Vaya a **NetScaler Gateway > Políticas > RDP** .
2. En la página **Perfiles y conexiones de RDP**, haga clic en la ficha **Perfiles de cliente** y seleccione el perfil de cliente en el que quiere configurar el atributo de enlace RDP.
3. En la página **Configurar perfil de cliente RDP**, en **Atributo de vínculo de RDP**, introduzca el nombre del atributo LDAP.

   Nota: El valor del atributo LDAP puede ser una lista separada por comas.

Aleatorizar el nombre del archivo RDP con el proxy RDP

March 27, 2024

Al hacer clic en una URL de RDP, se descarga un archivo RDP. Al volver a hacer clic en la **URL** RDP, se descarga un nuevo archivo RDP con el mismo nombre, lo que genera una ventana emergente para reemplazar el nuevo archivo por el archivo existente. Para evitarlo, el administrador puede optar por aleatorizar el nombre del archivo RDP. El nombre del archivo se ha aleatorizado agregando la salida de la función time () en el formato\ <rdpFileName\ >\ _\ <outputof time () >.rdp. De este modo, el dispositivo genera un nombre de archivo RDP único cada vez que descarga un archivo.

Configurar compatibilidad para la aleatorización de nombres de archivo RDP con proxy RDP

Para configurar la compatibilidad con la aleatorización de nombres de archivo RDP con proxy RDP mediante la interfaz de línea de comandos del símbolo del sistema, escriba:

```
1     add rdpclientprofile <profileName> -rdpfileName <filename> -
          randomizeRDPFilename <YES/NO>
2
3     add rdpclientprofile clientProfileName -rdpfileName testRDP -
          randomizeRDPFilename YES
4  <!--NeedCopy-->
```

Para configurar la compatibilidad con la aleatorización de nombres de archivo RDP con proxy RDP mediante la GUI de NetScaler:

1. ****Vaya a **NetScaler Gateway > Directivas > RDP** .**
2. En la página **Perfiles y conexiones RDP**, haga clic en la ficha **Perfiles de cliente** y seleccione el perfil de cliente en el que quiere configurar aleatoriamente la funcionalidad de nombre de archivo RDP.
3. En la página **Configurar perfil de cliente RDP**, seleccione **SÍ** en el menú junto al campo **Nombre de archivo RDP aleatorio**.

Configurar el nombre de los archivos RDP

March 27, 2024

Al descargar un archivo RDP, se puede almacenar localmente con el nombre de archivo configurado.

Configurar un nombre para los archivos RDP

Para configurar un nombre para los archivos RDP mediante la CLI, en la línea de comandos, escriba:**

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

Para configurar un nombre para los archivos RDP mediante la interfaz gráfica de usuario:

1. ****Vaya a **NetScaler Gateway > Directivas > RDP** .**
2. En la página **Perfiles y conexiones de RDP**, haga clic en la ficha **Perfiles de cliente**. Seleccione el perfil del cliente en el que quiere configurar una funcionalidad de nombre de archivo RDP aleatorio.
3. En la página **Configurar perfil de cliente RDP**, introduzca un nombre para el perfil RDP en el campo **Nombre de archivo RDP**. El nombre del archivo debe tener el siguiente formato,. Se permite un máximo de 31 caracteres para el nombre.

Compatibilidad con proxies ICA salientes

January 26, 2024

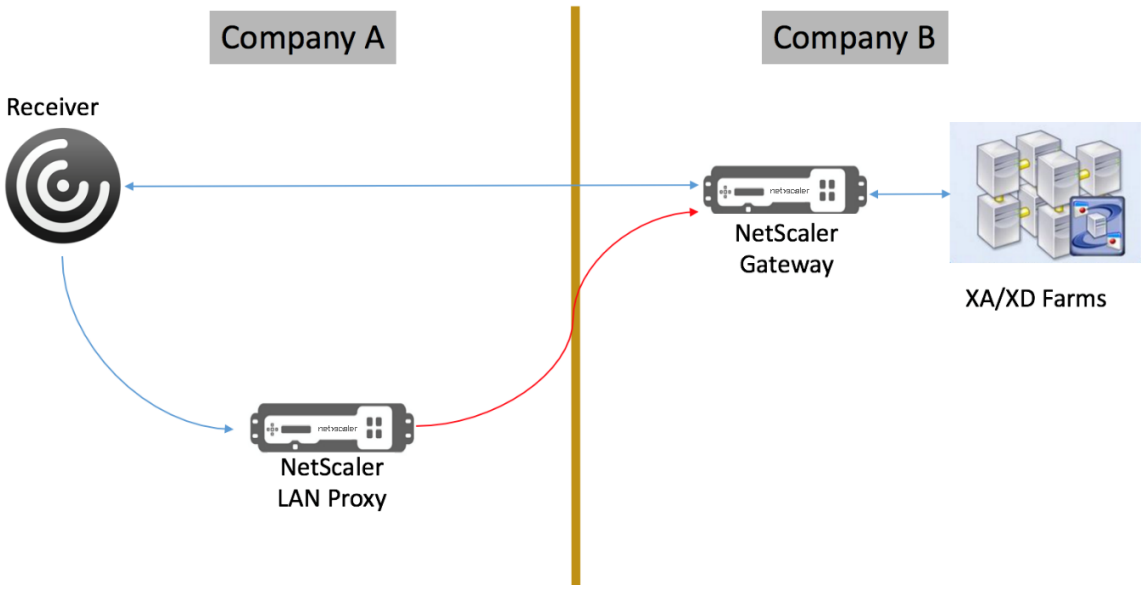
La compatibilidad con proxy ICA saliente para NetScaler Gateway permite a los administradores de red aprovechar las funcionalidades de SmartControl incluso cuando Receiver y NetScaler Gateway se implementan en distintas organizaciones.

En el siguiente caso se ilustra el uso de la solución Proxy ICA saliente:

Un administrador de red necesita controlar las capacidades relacionadas con la sesión ICA cuando Receiver y NetScaler Gateway se implementan en distintas organizaciones.

Comprensión de la compatibilidad con el proxy ICA saliente

Para llevar la funcionalidad de SmartControl a la organización empresarial, la empresa A, que tiene el receptor, necesitamos agregar un dispositivo NetScaler que actúe como proxy LAN. El proxy LAN de NetScaler aplica SmartControl y envía el tráfico a NetScaler Gateway de la empresa B. En este caso de implementación, Receiver reenvía el tráfico al proxy LAN de NetScaler, lo que permite que el administrador de red de la empresa A aplique SmartControl. La implementación se muestra en la siguiente ilustración.



En este caso, el tráfico entre el proxy LAN y NetScaler Gateway se realiza a través de SSL.

> **Nota:** No habilite la autenticación basada en certificados de cliente en NetScaler Gateway.

Compatibilidad con SSL en el proxy LAN de NetScaler

A partir de la versión 13.0 build xx.xx, el tráfico entre la aplicación Citrix Workspace y el proxy LAN de NetScaler también se admite a través de SSL. La aplicación Citrix Workspace cifra el tráfico que envía al proxy LAN a través de SSL. La compatibilidad con SSL en el proxy LAN puede coexistir con la implementación existente.

Para habilitar el cifrado de tráfico a través de SSL entre la aplicación Citrix Workspace y el proxy LAN de NetScaler, debe realizar lo siguiente en el proxy LAN de NetScaler:

- Inhabilite la autenticación y habilite el doble salto en el servidor virtual VPN.
- Establezca el host del cliente Windows en la dirección IP del servidor virtual VPN.
- Habilite la validación de certificados y SNI.
- Agregue los certificados de CA adecuados y actívalos de forma global.

Configuración del proxy ICA saliente

March 27, 2024

La configuración del proxy ICA saliente implica configurar el proxy LAN de NetScaler y NetScaler Gateway.

Configurar el proxy LAN de NetScaler para el proxy saliente ICA

Puede realizar los siguientes pasos para configurar el proxy ICA saliente mediante la CLI.

- Agregue un servidor virtual VPN.

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range <
    positive_integer>] [-ipset <string>]] [<port>] [-state (
    ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-
    doubleHop ( ENABLED |DISABLED )]
<!--NeedCopy-->
```

- Defina los parámetros de VPN.

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
    backendCertValidation ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

- Agrega un par de claves de certificado SSL.

```
add ssl certKey ca_cert_verify -cert <certificate name>
<!--NeedCopy-->
```

- Enlaza el par de claves de certificado SSL de forma global.

```
bind vpn global -cacert ca_cert_verify
<!--NeedCopy-->
```

Ejemplo:

```
- add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication
    OFF - doubleHop ENABLED

- set vpn parameter backendserverSni ENABLED backendcertValidation
    ENABLED

- add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer

- bind vpn global -cacert dnpg_ca

<!--NeedCopy-->
```

> **Nota:**
>
> Para la compatibilidad con SSL en el proxy LAN de NetScaler, no es necesario realizar cambios en la configuración de NetScaler Gateway.

Compatibilidad con proxy PCoIP habilitado para NetScaler Gateway para VMware Horizon View

January 26, 2024

NetScaler Gateway 12.0 admite el protocolo PC-over-IP (PCoIP), que es el protocolo de visualización remota de varias soluciones de VDI que no son de Citrix, incluida VMware Horizon View. PCoIP es análogo al protocolo Citrix HDX/ICA y al protocolo Microsoft RDP. PCoIP utiliza el puerto UDP 4172.

Cuando PCoIP se transmite mediante proxy a través de NetScaler Gateway, NetScaler Gateway puede reemplazar las soluciones de acceso remoto PCoIP tradicionales, como View Security Server o VMware Access Point.

En los siguientes casos se ilustra el uso de la solución VMware Horizon View habilitada para NetScaler Gateway.

- Usuarios de PCoIP de VMware Horizon que necesitan acceder de forma remota a grupos de escritorios y grupos de aplicaciones de VMware Horizon View a través de NetScaler Gateway sin implementar un servidor de seguridad de Horizon View ni un punto de acceso de VMware.
- Los usuarios de PCoIP acceden de forma remota a otras soluciones de escritorios virtuales basadas en PCoIP a través de NetScaler Gateway.

> **Nota**
>
> NetScaler Gateway se implementa como solución de acceso remoto.

Configurar el proxy PCoIP habilitado para NetScaler Gateway para VMware Horizon View

March 27, 2024

Requisitos previos

Versión: NetScaler 12.0 o superior

Licencia universal: PCoIP Proxy utiliza la función de acceso sin cliente de NetScaler Gateway, lo que significa que cada conexión de NetScaler Gateway debe tener licencia para NetScaler Gateway Universal. En el servidor virtual de NetScaler Gateway, asegúrese de que **solo ICA** esté desactivado.

Infraestructura de Horizon View: Una infraestructura interna de Horizon View funcional. Asegúrese de poder conectarse a Horizon View Agents internamente sin NetScaler Gateway. Asegúrese de que el **túnel seguro HTTP (S) de Horizon View y la SecureGateway PCoIP** no estén habilitados en los servidores de conexión de View a los que NetScaler realizará conexiones proxy.
Se admiten las siguientes versiones de VMware Horizon view.

- Servidor de conexión: 7.0.1 y superior
- Horizon Client: 4.2.0 y superior (Windows y Mac)

Puertos de firewall:

Asegúrese de lo siguiente:

- UDP 4172 y TCP 443 deben abrirse desde los clientes de Horizon View a la VIP de NetScaler Gateway.
- UDP 4172 debe estar abierto desde el SNIP de NetScaler a todos los agentes internos de Horizon View.
- El proxy PCoIP es compatible con NetScaler implementado detrás de NAT. Los siguientes son los puntos importantes a tener en cuenta:
  - La compatibilidad se basa en la configuración de parámetros FQDN del servidor virtual VPN
  - Solo admite FQDN de acceso público y no IP
  - Admite solo puertos 443 y 4172
  - Debe ser una NAT estática

Certificado: certificado válido para el servidor virtual de NetScaler Gateway.

Autenticación : directiva/servidor de autenticación LDAP que utiliza sintaxis avanzada.

Unified Gateway (opcional): Si Unified Gateway, cree la Unified Gateway antes de agregar la funcionalidad PCoIP.

Tema del portal RFWebUI : para el acceso del explorador web a Horizon View, el servidor virtual de NetScaler Gateway debe configurarse con el tema RFWebUI.

Horizon View Client: Horizon View Client debe instalarse en el dispositivo cliente, incluso si se accede a iconos publicados de Horizon mediante el portal NetScaler RfWebUI.

Para configurar NetScaler Gateway para que admita el proxy PCoIP para VMware Horizon View:

1. Vaya a **Configuración > Directivas de NetScaler Gateway > PCoIP**.
2. Cree un perfil de servidor virtual y un perfil PCoIP en la página **Perfiles y conexiones de PCoIP**.
   a) Para crear un perfil de servidor virtual, en la ficha **Perfiles de vServer**, haga clic en **Agregar**.

b) Escriba un nombre para el perfil del servidor virtual.

c) Introduzca un nombre de dominio de Active Directory que se utiliza para el inicio de sesión único en el servidor de conexión de View y, a continuación, haga clic en **Crear.**
Nota: Solo se admite un único dominio de Active Directory por servidor virtual de NetScaler Gateway. Además, el nombre de dominio especificado aquí se muestra en Horizon View Client.

d) Haga clic en **Login**.

e) Para crear un perfil PCoIP, en la ficha **Perfiles**, haga clic en **Agregar**.

   i. Introduzca un nombre para el perfil PCoIP.

   ii. Introduzca la URL de conexión del servidor de conexión de VMware Horizon View interno y, a continuación, haga clic en **Crear**.

f) Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.

g) A la derecha, selecciona la ficha **Perfiles de sesión**.

h) En la página **Perfiles y directivas de sesión de NetScaler Gateway**, cree o modifique un perfil de sesión de NetScaler Gateway.

   i. Para crear un perfil de sesión de NetScaler Gateway, haga clic en **Agregar**y escriba un nombre.

   ii. Para modificar un perfil de sesión de NetScaler Gateway, selecciónelo y haga clic en **Modificar**.

i) En la ficha **Experiencia del cliente**, asegúrese de que el valor **Acceso sin cliente** esté establecido **en On**.

j) En la ficha **Seguridad**, asegúrese de que el valor **Acción de autorización predeterminada** esté establecido en **PERMITIR**.

k) En la ficha **PCoIP**, seleccione el perfil PCoIP necesario y, a continuación, haga clic en **Crear**. También puede crear o modificar perfiles PCoIP desde esta ficha.

l) Haga clic en **Crear** o en **Aceptar** para terminar de crear o modificar el perfil de sesión.

m) Si ha creado un perfil de sesión, también debe crear una directiva de sesión correspondiente.

   i. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.

   ii. seleccione la ficha **Directivas de sesión** y luego haga clic en **Agregar**.

   iii. En la página Crear directiva de sesión de NetScaler Gateway, introduzca un nombre para la directiva.

   iv. En **Perfil**, seleccione un perfil existente o haga clic en **Agregar** y cree un perfil.

v. Agregue una expresión.

A. Haga clic en **Directiva avanzada** y, después, en **Editor de expresiones**.
B. En **Expresión**, seleccione la expresión según sus requisitos.

vi. Haga clic en **Aceptar.**

n) Enlazar el perfil del servidor virtual PCoIP y la directiva de sesión creados a un servidor virtual NetScaler Gateway.

i. Vaya a **NetScaler Gateway > Servidores virtuales**.

ii. A la derecha, **agregue** un nuevo servidor virtual de NetScaler Gateway o **modifique** un servidor virtual de NetScaler Gateway existente.

iii. Si modifica un servidor virtual de NetScaler Gateway existente, en la sección **Configuración básica**, haga clic en el icono de lápiz.

iv. Para agregar y modificar, en la sección **Configuración básica**, haga clic en **Más**.

v. Utilice el menú **Perfil de vServer de PCoIP** para seleccionar el perfil de servidor virtual PCoIP necesario.

vi. Desplácese hacia abajo y asegúrate de que solo ICA esté desactivada. A continuación, haga clic en **Aceptar** para cerrar la sección **Configuración básica**.

vii. Si va a crear un servidor virtual de NetScaler Gateway, vincule un **certificado**y una directiva de autenticación LDAP.

viii. Desplácese hacia abajo hasta la sección **Directivas** y haga clic en el icono más.

ix. El valor predeterminado de la página **Elegir tipo** es **Sesión** y **Solicitud**. Haga clic en **Continuar**.

x. En la sección **Vinculación de directivas**, haga clic **en Haga clic para seleccionar**.

xi. Seleccione la directiva de sesión necesaria que tiene configurado el perfil PCoIP y haga clic en **Seleccionar**.

xii. En la página **Vinculación de directivas**, haga clic en **Vincular**.

xiii. Si desea utilizar un explorador web para conectarse a VMware Horizon View, en **Configuración avanzada**, agregue la sección **Temas del portal**. Si solo usa Horizon View Client para conectarse a NetScaler Gateway, no debe realizar este paso.

xiv. Utilice el menú **Tema del portal** para seleccionar **RfWebUI** y haga clic en **Aceptar**.

xv. Los iconos publicados de Horizon View se agregan al portal de RfWebUI.

> **Nota:** VMware utiliza dos o más protocolos cuando utiliza cualquier protocolo que no sea RDP. Esto puede hacer que las solicitudes tengan un equilibrio de carga en dos servidores back-end diferentes. Puede resolver este problema configurando un único grupo de persistencia en todos los protocolos para garantizar que todas las conexiones permanezcan en el mismo servidor virtual Citrix.

Pasos para habilitar la redirección USB

Se puede acceder a los dispositivos USB conectados a la máquina cliente desde los escritorios virtuales y las aplicaciones. A continuación se indican los pasos para habilitar la redirección USB:

1. Inicie sesión en la consola de administrador de VMware Horizon.
2. Vaya a **Inventario > Ver servidores de configuración**.
3. Seleccione la ficha **Servidores de conexión**.
4. Seleccione un servidor de conexión de la lista y haga clic en **Modificar**.
5. En la ficha **General**, seleccione la opción **Usar conexión de túnel seguro a máquina** en **HTTP (S) Secure Tunnel**. Proporcione la URL externa de NetScaler Gateway en el campo **URL externa**.

Actualización de la expresión de cambio de contenido para Unified Gateway

Si el servidor virtual de NetScaler Gateway está detrás de Unified Gateway (servidor virtual de conmutación de contenido), debe actualizar la expresión de conmutación de contenido para incluir las rutas de URL de PCoIP.

1. En la GUI de NetScaler, vaya a **Configuración > Administración del tráfico > Cambio de contenido > Directivas**.
2. Agregue la siguiente expresión en el área **Expresión** y, a continuación, haga clic en **Aceptar**.

	http.req.url.path.eq (“/broker/xml”)	http.req.url.path.contains (“/broker/resources”)	http.req.url.path.eq (“/pcoip-client”)

Usar puerta de enlace PCoIP

1. Para conectarse, debe tener Horizon View Client instalado en el dispositivo cliente. Una vez instalado, puede usar la interfaz de usuario de Horizon View Client para conectarse a NetScaler Gateway o puede usar la página del portal RFWebUI de NetScaler Gateway para ver los iconos publicados desde Horizon.

2. Para ver las conexiones PCoIP activas, vaya a **NetScaler Gateway > PCoIP.**
3. A la derecha, cambia a la ficha **Conexiones**. Las sesiones activas se muestran con los siguientes datos: nombre de usuario, IP de cliente de Horizon View e IP de destino de Horizon View Agent.
4. Para terminar una conexión, haga clic con el botón derecho en la ficha **Conexión** y haga clic **en Eliminar conexión**. O haga clic en **Matar todas las conexiones** para terminar todas las conexiones PCoIP.

Configurar el servidor de conexión de VMware Horizon View

January 26, 2024

Para admitir el proxy PCoIP a través de NetScaler Gateway:

1. Inicie sesión en la **consola de administrador de VMware Horizon**.
2. Vaya a **Inventario** —> **Ver configuración** —> **Servidores**.
3. Seleccione la ficha **Servidores de conexión**.
4. Seleccione un servidor de conexión de la lista y haga clic en **Modificar**.
5. En la ficha **General**, anule la selección de la opción **Usar conexión de túnel seguro** a máquina en HTTP(S) Secure Tunnel.
6. Haga clic en **Aceptar** para cerrar la ventana **Modificar configuración del servidor de conexión**.
7. Siga los pasos del 4 al 6 en todos los servidores de conexión de la lista.

Configuración automática de proxy para proxy saliente compatible con NetScaler Gateway

January 26, 2024

Al configurar el dispositivo NetScaler Gateway para que admita la configuración automática de proxy (PAC), la dirección URL de un archivo PAC se inserta en el explorador del cliente. El tráfico del cliente se redirige a los servidores proxy respectivos según las condiciones definidas en el archivo PAC.

A continuación se presentan algunos casos de uso comunes de PAC para proxy saliente:

- Configurar varios servidores proxy que gestionan el tráfico de clientes.
- Equilibrar la carga del tráfico del proxy en las subredes.

Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la CLI

En la línea de comandos, escriba:

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

Configurar NetScaler Gateway para que admita PAC en un perfil de sesión mediante la CLI

En la línea de comandos, escriba:

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

Donde:

- **URL**: URL del servidor proxy
- **Nombre**: Nombre de la acción de sesión de VPN

Configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Configuración global**.
2. En la página **Configuración global**, haga clic en **Cambiar configuración global** y, a continuación, seleccione la **ficha Experiencia del cliente**.
3. En la ficha**Experiencia del cliente**, seleccione**Configuración avanzada**y, a continuación, seleccione la**ficha Proxy**.
4. En la**ficha Proxy**, seleccione **Explorador** y, a continuación, seleccione **Usar configuración automática**.
5. En el campo**URL al archivo de configuración automática del proxy**, escriba la URL del archivo PAC necesario.
6. Haga clic en **Create**.

Configurar NetScaler Gateway para que admita PAC en el perfil de sesión mediante la interfaz gráfica de usuario

1. Vaya a **Configuración > NetScaler Gateway > Directivas > Sesión**.
2. En la página **Perfiles y directivas de sesión**de NetScaler Gateway, cree un perfil de sesión de NetScaler Gateway.

3. Seleccione la ficha **Perfiles de sesión**, haga clic en **Agregar**e introduzca un nombre.
4. En la ficha **Experiencia del cliente**, seleccione **Configuración avanzada** y, a continuación, seleccione la ficha **Proxy**.
5. En la ficha **Proxy**, seleccione **Explorador** y, a continuación, seleccione **Usar configuración automática**.
6. En el campo**URL al archivo de configuración automática del proxy**, escriba la URL del archivo PAC necesario.
7. Haga clic en **Create**.
8. Haga clic en **Create**.

Compatibilidad de configuración para el atributo de cookie SameSite

March 27, 2024

El atributo `SameSite` indica al explorador si la cookie se puede utilizar para el contexto entre sitios o solo para el contexto del mismo sitio. Si se pretende acceder a una aplicación en el contexto entre sitios, solo puede hacerlo a través de la conexión HTTPS. Para obtener más información, consulte RFC6265.

Hasta febrero de 2020, el atributo `SameSite` no se establecía explícitamente en el dispositivo NetScaler. El explorador tomó el valor predeterminado (Ninguno). La falta de configuración del atributo `SameSite` no afectó a las implementaciones de NetScaler Gateway y NetScaler AAA.

Con la actualización de ciertos exploradores, como Google Chrome 80, se produce un cambio en el comportamiento predeterminado entre dominios de las cookies. El atributo `SameSite` se puede establecer en uno de los valores siguientes. El valor predeterminado para Google Chrome se establece en Lax. Para determinadas versiones de otros exploradores, el valor predeterminado del atributo `SameSite` puede estar establecido en Ninguno.

- **Ninguno**: indica el explorador que utilizará la cookie en el contexto entre sitios solo en conexiones seguras.
- **Lax**: indica el explorador que utilizará la cookie para las solicitudes en el mismo contexto del sitio. En el contexto entre sitios, solo los métodos HTTP seguros como la solicitud GET pueden usar la cookie.
- **Estricto**: utiliza la cookie solo en el mismo contexto del sitio.

Si no hay ningún atributo `SameSite` en la cookie, Google Chrome asume la funcionalidad de `SameSite` = Lax.
Como resultado, para las implementaciones dentro de un iframe con contexto entre sitios que requieren que el explorador inserte cookies, Google Chrome no comparte cookies entre sitios. Como resultado, es posible que el iframe del sitio web no se cargue.

Configurar el atributo de cookie SameSite

Se agrega un nuevo atributo de cookie denominado SameSite a los servidores virtuales VPN y NetScaler AAA. Este atributo se puede establecer a nivel global y a nivel de servidor virtual.

Para configurar el atributo SameSite, debe realizar lo siguiente:

1. Establecer el atributo SameSite del servidor virtual
2. Enlazar las cookies al patset (si el explorador deja caer las cookies entre sitios, el explorador las deja caer)

Configuración del atributo SameSite mediante la CLI

Para establecer el atributo SameSite en el nivel del servidor virtual, utilice los siguientes comandos.

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

Para establecer el atributo SameSite a nivel global, utilice los siguientes comandos.

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

Nota: La configuración del nivel del servidor virtual tiene preferencia sobre la configuración de nivel global. Citrix recomienda configurar el atributo de cookies SameSite en el nivel del servidor virtual.

Vinculación de cookies a patset mediante la CLI

Si el explorador deja caer cookies entre sitios, puede enlazar esa cadena de cookie a la existente para ns_cookies_SameSite patset que el atributo SameSite se agregue a la cookie.

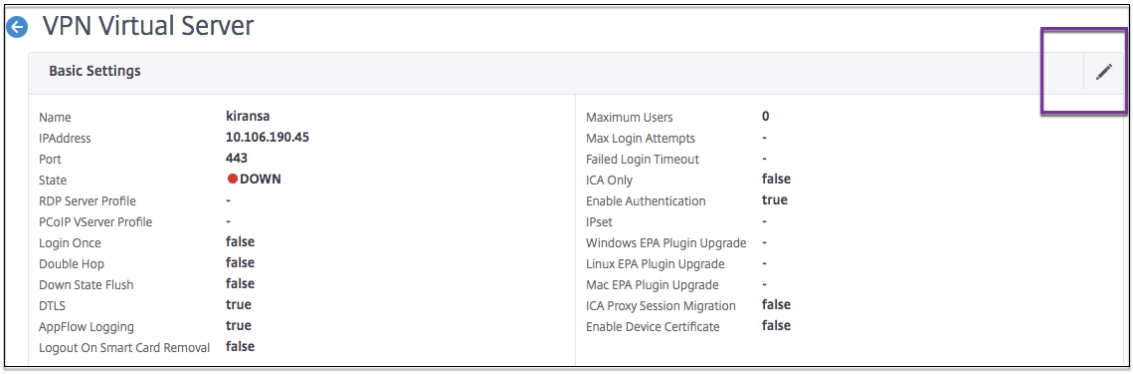
Ejemplo:

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

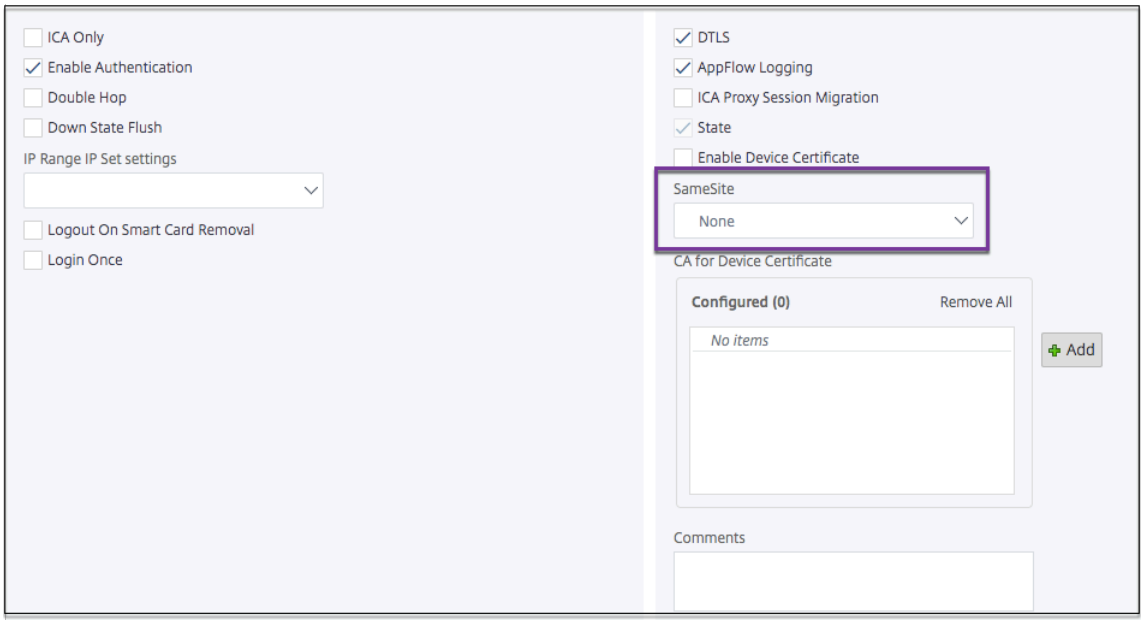
Configuración del atributo sameSite mediante la interfaz gráfica de usuario

Para establecer el atributo SameSite en el nivel del servidor virtual:

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. Seleccione un servidor virtual y haga clic en **Modificar**.
3. Selecciona el icono de modificación en la sección **Configuración básica** y haga clic en **Más**.

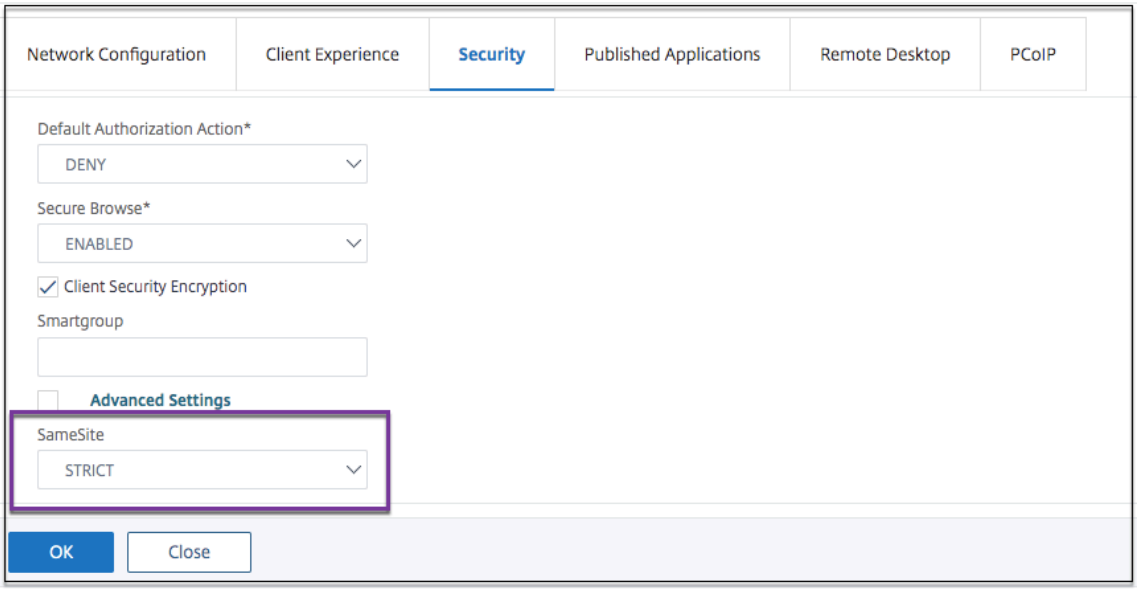


4. En **SameSite**, seleccione la opción según sea necesario.



Para definir el atributo `SameSite` a nivel global:

1. Vaya a **NetScaler Gateway > Configuración global > Cambiar configuración global .**
2. Haga clic en la ficha **Seguridad**.
3. En **`SameSite`**, seleccione la opción según sea necesario.



Configuración de RfWebUI Persona on Gateway UX

March 27, 2024

RfWebUI Persona es un tema que proporciona una nueva página de inicio de sesión y portal para los usuarios de NetScaler Gateway que inician sesión a través de NetScaler Gateway. El portal presenta a los usuarios de Receiver, StoreFront y Citrix Endpoint Management la misma interfaz gráfica de usuario que cuando acceden directamente a uno de esos productos.

Cuándo usar RfWebUI Persona

Utilice el personaje RFWebUi en NetScaler Gateway cuando necesite una vista de panel único de todas las aplicaciones que proporcionan los diferentes productos de NetScaler, como las aplicaciones web y de software como servicio (SaaS), las aplicaciones virtuales de Windows y los escritorios.

Los siguientes casos ilustran el uso de RfWebUI Persona.

- Un usuario accede a StoreFront mediante Gateway y encuentra una interfaz gráfica de usuario diferente a la que ve al acceder al producto sin Gateway.
  Solución: Cuando el usuario accede a StoreFront mediante la puerta de enlace, el tema RfWebUI proporciona una interfaz de usuario similar a la que ve al acceder al producto sin utilizar la puerta de enlace.
- Un usuario accede a las aplicaciones Citrix Workspace, StoreFront y Citrix Endpoint Management mediante Gateway y tiene dificultades para localizar las aplicaciones deseadas, ya que

las aplicaciones no están agrupadas de forma lógica.
Solución: La persona RfWebUI proporciona una experiencia de usuario de vista de panel único mediante la creación de un paquete lógico de aplicaciones proporcionadas por diferentes productos, como Receiver, StoreFront, Citrix Endpoint Management, etc.

Funcionalidades proporcionadas por RfWebUI Persona

El nuevo RfWebUI ofrece las siguientes funciones:

- IR
- Agregación de aplicaciones
- Enlaces proxy del Protocolo de escritorio remoto (RDP) configurado por el usuario
- Aplicaciones favoritas

IR

GO: La función Go proporciona acceso a las páginas web a través de una VPN sin cliente. El usuario simplemente escribe la URL en la sección **URL** de la ficha **Marcadores** y hace clic en **IR**.

Actualmente, la función **GO** solo admite Outlook Web Application (OWA) y direcciones URL de SharePoint.

> **Nota**
> La ficha **GO** solo está visible si el parámetro `clientlessAccessVPNMode` de la directiva de sesión está **Habilitado**.

Agregación de aplicaciones

Agregación de aplicaciones: El tema RfWebUI proporciona una vista de panel único al agrupar las aplicaciones proporcionadas por diferentes productos bajo banners descriptivos. Por ejemplo, todas las URL de VPN configuradas por un administrador de NetScaler se encuentran en un paquete denominado **Aplicaciones web y SaaS**, y los marcadores web específicos del usuario se encuentran en **Marcadores personales**. Si los paquetes de aplicaciones de Citrix Virtual Apps and Desktops están configurados en StoreFront, la vista de panel único de NetScaler Gateway también incluye estos paquetes.

Vínculos proxy de RDP configurados

Los usuarios pueden agregar un enlace de proxy RDP como marcadores personales. Los marcadores personales aparecen en la ficha **Escritorios**.

Se admiten los siguientes modos RDP:

- Puerta de enlace única
- Puerta de enlace sin estado (doble)

> **Nota:** Un usuario solo puede agregar vínculos proxy RDP si `RDPclientprofile` se ha configurado un. Para obtener más información sobre las configuraciones de RDP, consulte la documentación del proxy RDP .

Aplicaciones favoritas

Los usuarios pueden agregar las aplicaciones deseadas que aparecen en **Aplicación web y SaaS** y en **Marcadores personales** a la ficha **FAVORITOS** haciendo clic en el enlace **Agregar a favoritos** que aparece junto al nombre de la aplicación. Las aplicaciones una vez agregadas se pueden ver en la ficha **FAVORITOS**. Lo mismo también se puede quitar de la ficha **FAVORITOS** haciendo clic en el enlace **ELIMINAR** presente junto a la aplicación dentro de la ficha **FAVORITOS**.

Consideraciones al habilitar la persona RfWebUI

La persona de RfWebUI no es totalmente compatible con lo siguiente:

Función de uso compartido de archivos: no se admite la función de uso compartido de archivos SMB para acceder a recursos compartidos de archivos SMB.
Inicio de correo electrónico: El parámetro VPN de **correo electrónico principal** no está disponible como vista incrustada para el portal de NetScaler Gateway. Se puede acceder a él como una aplicación en el paquete de **aplicaciones web y SaaS** en la ficha **APPS** de RfWebUI.
Cliente Java: El cliente Java basado en explorador para establecer un túnel SSL no está disponible en este tema.

Configuración de RfWebUI Persona

Para aplicar la Persona RfWebUI:

1. En la interfaz de NetScaler, vaya a **Configuración > Temas del portal de NetScaler Gateway**.
2. En la página **Temas del portal**, seleccione la casilla de verificación **RfWebUI**.
3. Haga clic en el icono **Guardar** en la esquina superior derecha de la página **Temas del portal**.
4. En el cuadro de diálogo **Guardar confirmación**, haga clic en **Sí**.

Parámetros de configuración de RFWebUI

March 27, 2024

Dos archivos de configuración influyen en el comportamiento general del portal de NetScaler Gateway: el archivo de configuración local de NetScaler Gateway y el archivo StoreFront.

En función de la implementación, puede modificar el comportamiento del portal de NetScaler Gateway cambiando las propiedades del archivo "plugins.xml". Este fichero aparece como fichero de configuración en el explorador del que se solicita `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

Durante el inicio de sesión, se utilizan los archivos de configuración de NetScaler Gateway. Sin embargo, cuando se conecta a StoreFront, StoreFront envía una nueva configuración y se sobrescribe la configuración anterior. Este comportamiento es diferente para la VPN sin cliente y la ICA.

Para ICA, la configuración de StoreFront siempre tiene prioridad, pero algunos de los comportamientos de la VPN sin cliente en los que influye la configuración de NetScaler Gateway se conservan incluso después de actualizar la nueva configuración desde StoreFront.

En la tabla siguiente se enumeran los parámetros que describen la configuración que tiene prioridad sobre la VPN sin cliente y la ICA.

Tipo de configuración	sub config type	Parámetro	VPN sin cliente	ICA	Descripción
Sesión para VPN sin cliente/AuthManager para ICA	-	loginFormTimeout	NetScaler Gateway	-	Define el tiempo en minutos para el tiempo de espera de la página de inicio de sesión
Asistente de plug-ins	-	enabled	StoreFront	StoreFront	Habilitar o inhabilitar el asistente de plug-ins
Asistente de plug-ins	-	upgradeAtLogin	StoreFront	StoreFront	Solicita la actualización del plug-in al iniciar sesión
Asistente de plug-ins	-	showAfterLogin	NetScaler Gateway	StoreFront	Muestra el mensaje del plug-in después de iniciar sesión

Tipo de configuración	sub config type	Parámetro	VPN sin cliente	ICA	Descripción
Asistente de plug-ins	-	showOnlyIfRequiredByApps	NetScaler Gateway	StoreFront	Muestra el mensaje del plug-in después de iniciar sesión, si las aplicaciones lo requieren
Asistente de plug-ins	macOS/win32	path	NetScaler Gateway	StoreFront	Define la ruta de descarga de los plug-ins
Asistente de plug-ins	protocolHandler	enabled	NetScaler Gateway	StoreFront	Activa o desactiva la página del controlador de protocolos antes de iniciar el plug-in
Asistente de plug-ins	protocolHandler	platforms	NetScaler Gateway	StoreFront	Identifica la plataforma admitida para el plug-in
Asistente de plug-ins	-	skipDoubleHopCheckWhenDisabled	NetScaler Gateway	StoreFront	Activa o desactiva la comprobación de configuración de doble salto de NetScaler Gateway para el paso ICA
Interfaz de usuario	-	frameOptions	NA	NA	-

Tipo de configuración	sub config type	Parámetro	VPN sin cliente	ICA	Descripción
Interfaz de usuario		autoLaunchDesktop	StoreFront	StoreFront	Habilita o inhabilita el inicio del escritorio
Interfaz de usuario	workspaceControl	enabled	StoreFront	StoreFront	Activa o desactiva el control del espacio de trabajo
Interfaz de usuario	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	Activa o desactivar la reconexión automática de la sesión anterior si está disponible
Interfaz de usuario	workspaceControl	logoffAction	StoreFront	StoreFront	Define el comportamiento de cierre de sesión de Citrix Workspace
Interfaz de usuario	workspaceControl	showReconnectButton	StoreFront	StoreFront	Muestra u oculta el botón **Reconectar**
Interfaz de usuario	workspaceControl	showDisconnectButton	StoreFront	StoreFront	Muestra u oculta el botón **Desconectar**
Interfaz de usuario	workspaceControl	showDesktopsView	StoreFront	StoreFront	Muestra u oculta la vista Escritorios
Interfaz de usuario	workspaceControl	showAppsView	StoreFront	StoreFront	Muestra u oculta la vista Aplicaciones

Tipo de configuración	sub config type	Parámetro	VPN sin cliente	ICA	Descripción
Interfaz de usuario	workspaceControl	defaultView	StoreFront	StoreFront	Selecciona la vista Escritorio o la vista Aplicación
Interfaz de usuario	receiverConfiguration	enabled	StoreFront	StoreFront	Activa o desactiva la configuración del receptor
Interfaz de usuario	receiverConfiguration	showOnlyIfRequiredByApps	NetScaler Gateway	NetScaler Gateway	Muestra el mensaje del receptor si las aplicaciones lo requieren
Interfaz de usuario	receiverConfiguration	downloadURL	StoreFront	StoreFront	Descarga la URL del receptor
Interfaz de usuario	appShortcuts	enabled	StoreFront	StoreFront	Activa o desactiva la ficha de acceso directo de la aplicación
Interfaz de usuario	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	Permitir la reconexión de sesiones

Personalización del portal de puerta de enlace mediante plug-ins personalizados

March 27, 2024

El marco RfWebUI de NetScaler Gateway ofrece la posibilidad de agregar los plug-ins personalizados para personalizar su portal de puerta de enlace. Estos plug-ins personalizados se pueden utilizar para

agregar una gran funcionalidad a la puerta de enlace, por ejemplo, si quiere agregar una página completamente nueva en el flujo de la puerta de enlace. Para otros casos de uso, el código se puede agregar al archivo de script personalizado proporcionado para los temas de puerta de enlace en la ubicación /var/netscaler/logon/themes/<custom_theme>/script.js.

1. Para agregar un plug-in personalizado, cree el archivo JavaScript en la ubicación /var/netscaler/logon/LogonPoint/plugins/ns-gateway/. Por ejemplo, puede encontrar los siguientes plug-ins en /var/netscaler/logon/LogonPoint/plugins/ns-gateway/.

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   Se recomienda introducir el nombre del plug-in con el formato <plugin_name>.js.

   Todos estos archivos de plug-ins se obtienen mediante el marco RfWebUI requerido por la funcionalidad.

2. Después de crear el archivo de plug-in, utilice el siguiente código como ejemplo para registrar el plug-in con el marco RfWebUI.

```
1          (function ($) {
2
3                      CTXS.ExtensionAPI.addPlugin( {
4
5                                  Name : “plugin name”,
6                                  initialize: function() {
7    }
8
9                       }
10  );
11              }
12  )(jQuery);
13 <!--NeedCopy-->
```

   donde,

   name es el nombre que se le da al plug-in. Se utiliza como identificador del plug-in.

   initialize toma la función como parámetro que se utiliza para inicializar el plug-in.

3. Introduzca el nombre del plug-in y la función de inicialización en la función CTXS.ExtensionAPI.addPlugin() para registrar el plug-in.
   El nombre y la ubicación del plug-in agregado deben estar registrados en el archivo plugins.xml de la ubicación /var/netscaler/logon/themes/<custom_theme>/plugins.xml.

4. Después de escribir el código del plug-in, el nombre y la ubicación del plug-in recién agregado deben registrarse con el archivo plugins.xml en la ubicación /var/netscaler/logon

/themes/<custom_theme>/plugins.xml. El plug-in debe estar registrado con la etiqueta plug-in.

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
   .js"/>
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"
   />
</plugins>
<!--NeedCopy-->
```

5. Introduzca un nombre y src para el plug-in para que rfWebUI pueda identificar y recuperar el plug-in.

Ejemplo de configuración

Las configuraciones de ejemplo siguientes se pueden utilizar para agregar un plug-in personalizado para agregar un pie de página a la página de inicio de sesión de NetScaler Gateway.

1. Cree el archivo de plug-in de JavaScript en la ubicación, /var/netscaler/logon/LogonPoint/plugins/ns-gateway/.
2. Asigne al plug-in el nombre ns-footer.js /var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js
3. Agregue el siguiente código al plug-in registrado en la RfWebUI y en la función de inicialización agregue el pie de página a la puerta de enlace.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
        configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='
               text-align:center;color:white;font-size:15px;'><br>
               Disclaimer<BR><BR>"+
                " Access to this website is restricted to
                   employees of Login Consultants<BR></div>");
            callback();
         }
;
     }

}
```

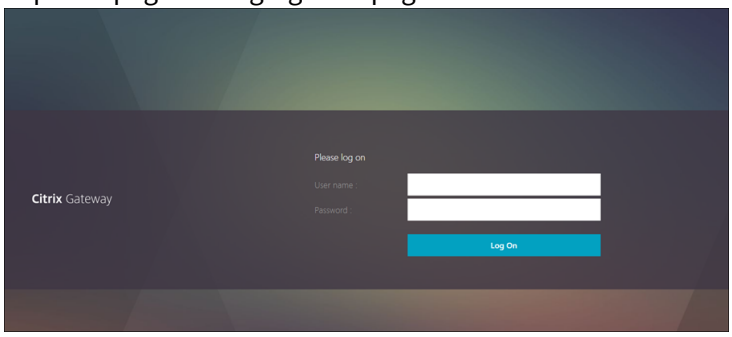


```
18   );
19   }
20   )(jQuery);
21  <!--NeedCopy-->
```

4. Guarde el archivo.
5. Agregue el nombre y src en el archivo plugins.xml de la ubicación `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
1  <plugins>
2  <plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
3  <plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
       .js" />
4  <plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js"
       />
5  <plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
6  </plugins>
7  <!--NeedCopy-->
```

6. Configure el tema personalizado para el que se agrega el plug-in.
7. Limpia la caché con el comando `flush cache contentgroup loginstaticobjects` .
8. Vuelva a cargar la pantalla del portal.
   El pie de página se agrega a la página de inicio de sesión de NetScaler Gateway.



Crear y personalizar el esquema de inicio de sesión

January 26, 2024

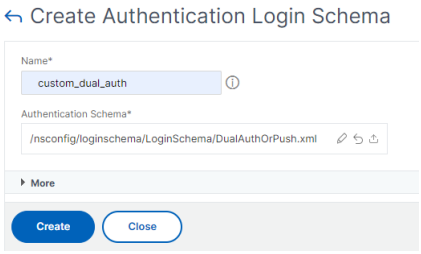
Esquema de inicio de sesión es el archivo XML que proporciona la estructura de la autenticación basada en formularios.
Los usuarios pueden utilizar una amplia gama de formularios de autenticación mediante un conjunto de construcciones de interfaz de usuario similares a los formularios HTML básicos.

En las autenticaciones nFactor, los factores de autenticación están encadenados entre sí. Cada factor puede tener páginas o archivos de esquema de inicio de sesión diferentes. En algunos casos de autenticación, a los usuarios se les pueden presentar varias pantallas de inicio de sesión. También puede hacer que un esquema de inicio de sesión recopile la información que se puede transmitir a varios factores para que estos últimos factores no tengan que mostrar otro esquema de inicio de sesión.

Los archivos XML del esquema de inicio de sesión se incluyen en el dispositivo NetScaler de `/nsconfig/loginschema/LoginSchema`.

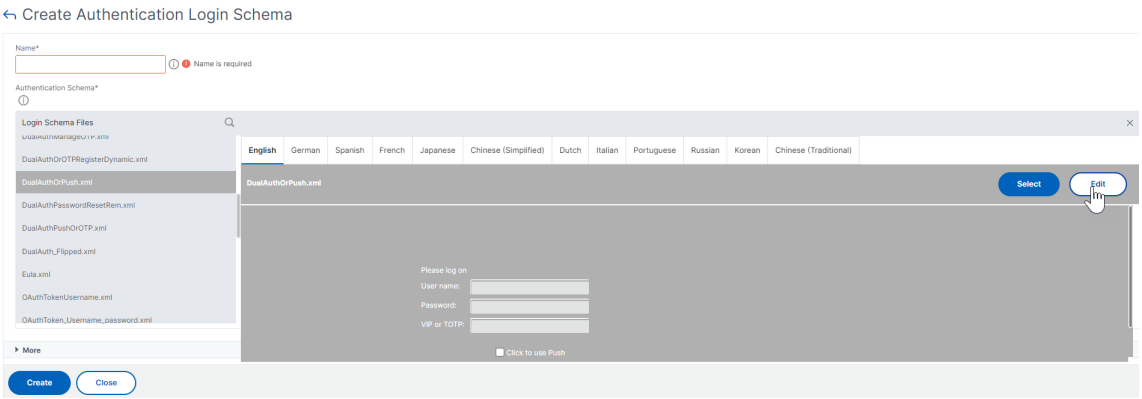
Crear un perfil de esquema de inicio de sesión

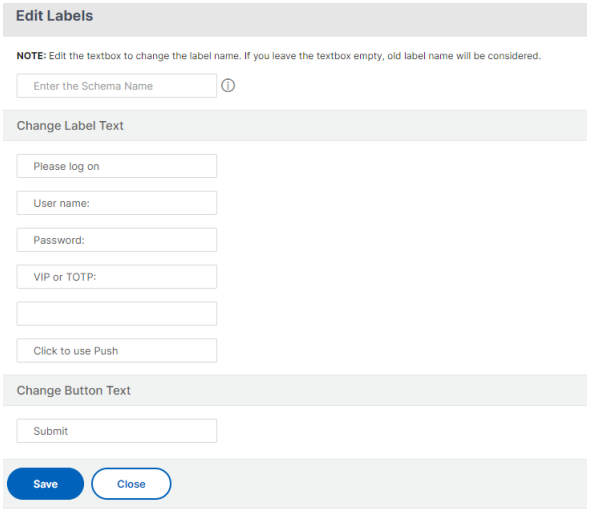
1. Vaya a **Seguridad > AAA: Tráfico de aplicaciones > Esquema de inicio**de sesión.
2. Haga clic en la ficha **Perfiles** y, a continuación, haga clic en **Agregar**.
3. En **Esquema de autenticación**, haga clic en el icono del lápiz.



4. Haga clic en la carpeta **LoginSchema** para ver los archivos que contiene.
5. Seleccione uno de los archivos y realice los cambios necesarios.

    - Cambia las etiquetas haciendo clic en el botón Modificar en la parte superior derecha.
    - Modifique el esquema seleccionando el idioma.

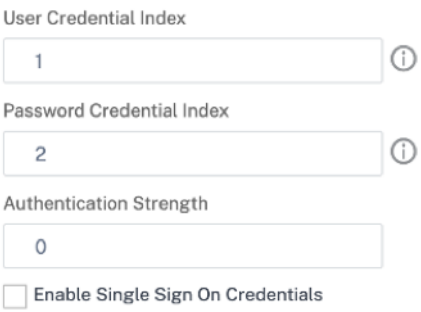


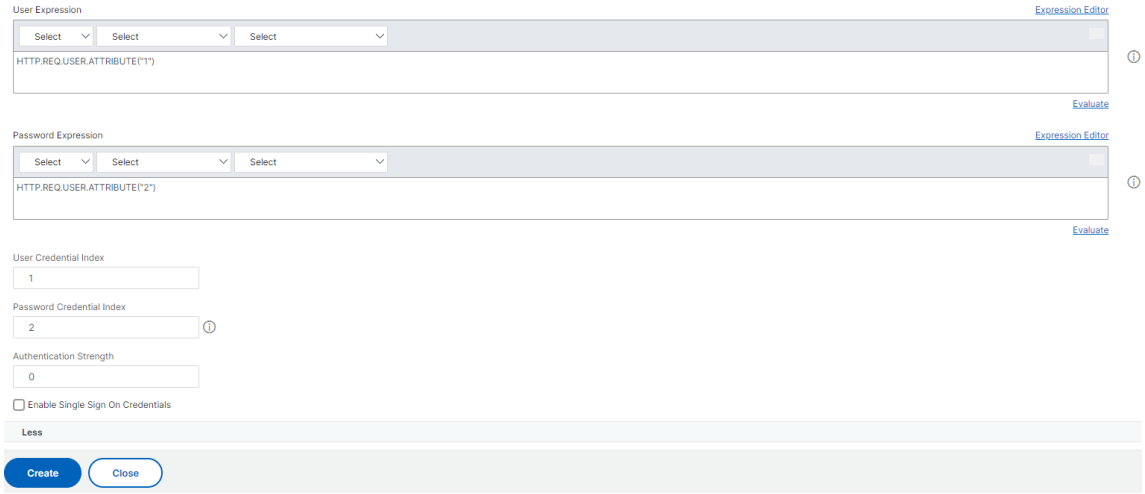


Nota: Al guardar los cambios tras la modificación, se crea un nuevo archivo XML de esquema con los cambios.

6. En la parte superior derecha, haga clic en **Seleccionar** para seleccionar el esquema XML modificado.
7. Introduzca un nombre de esquema de inicio de sesión y haga clic en **Más**.

   Nota: Puede utilizar las credenciales ya introducidas en otros lugares. Por ejemplo, puede utilizar el nombre de usuario y una de las contraseñas para el inicio de sesión único en StoreFront. Puede hacer clic en **Más** e introducir valores únicos para los índices. Estos valores pueden estar entre 1 y 16. Puede hacer referencia a estos valores de índice en una directiva de tráfico o un perfil mediante la expresión REQ.USER.ATTRIBUTE (#).





8. Haga clic en **Crear** para crear el perfil de esquema de inicio de sesión.

Enlazar un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría

Para enlazar un perfil de esquema de inicio de sesión a un servidor virtual de autenticación, autorización y auditoría, primero debe crear una directiva de esquema de inicio de sesión. Las directivas de esquema de inicio de sesión no son necesarias cuando se vincula el perfil del esquema de inicio de sesión a una etiqueta de directiva de autenticación.

Para crear y enlazar una directiva de esquema de inicio de sesión:

1. Vaya a **Seguridad > AAA > Esquema de inicio**de sesión.
2. Haga clic en la ficha **Directivas** y, a continuación, haga clic en **Agregar**.
3. En **Perfil**, seleccione el perfil de esquema de inicio de sesión creado anteriormente.
4. En **Regla**, introduzca la expresión de sintaxis predeterminada y haga clic en **Crear**.

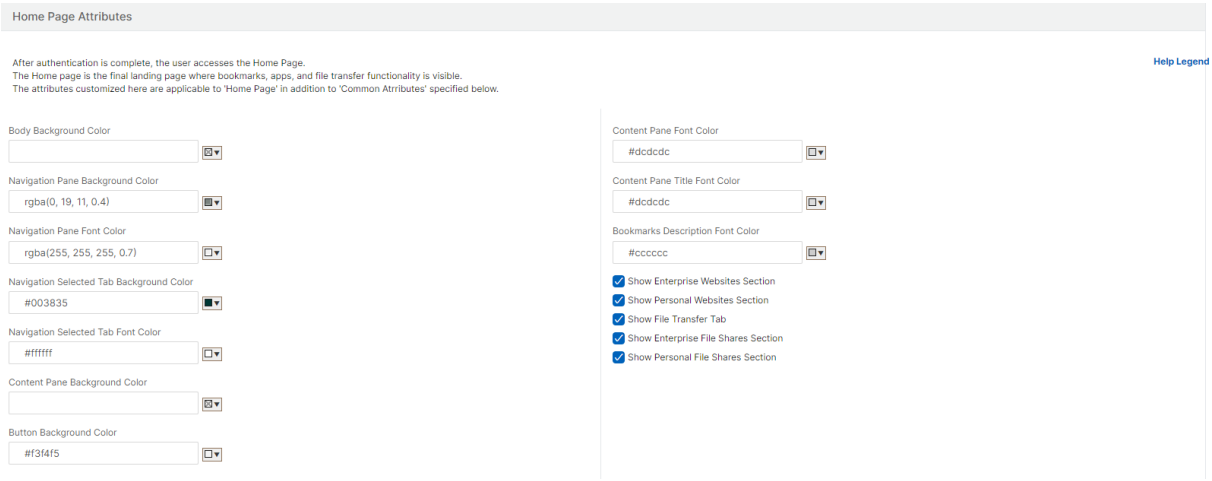
Personalizaciones del portal desde la interfaz de usuario de administración

January 26, 2024

Los administradores pueden personalizar los temas del portal creando los temas personalizados para lograr la apariencia personalizada del portal del usuario. Se pueden crear temas personalizados basados en los temas RfWebUI, Default, X1 y GreenBubble.

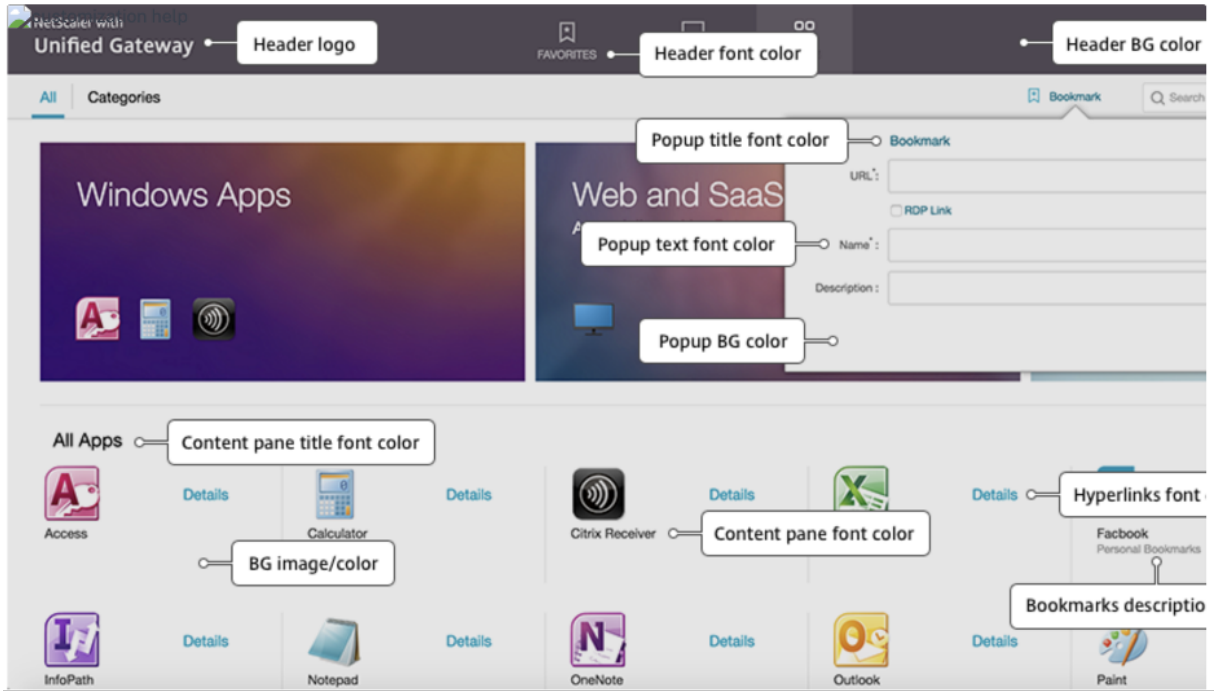
Para crear los temas personalizados:

1. En la ficha Configuración, vaya a **NetScaler Gateway > Temas del portal** y haga clic en **Agregar**.
2. Introduzca un nombre para el nombre del tema personalizado.
3. En **Tema de plantilla**, seleccione el tema base, según sus necesidades. **RfWebUI** se selecciona de forma predeterminada.
4. Haga clic en **Aceptar**.
5. En la sección **Apariencia**, modifique los atributos según sus requisitos para la página de inicio y haga clic en **Aceptar**.



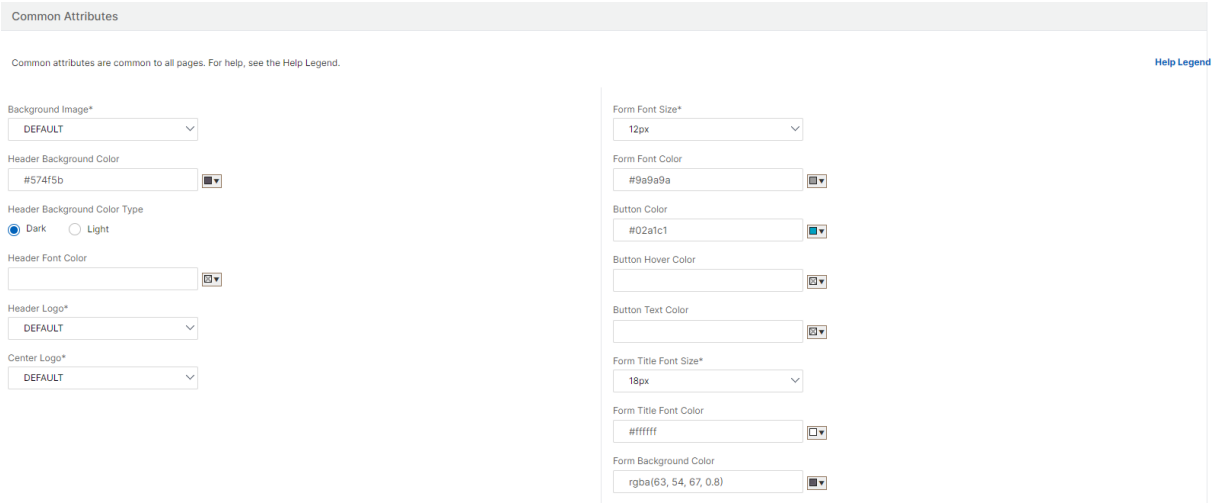
La siguiente ilustración muestra el tema personalizado basado en RfWebUi.

El enlace **Leyenda de ayuda** muestra la visualización gráfica de la página con los nombres de las secciones para ayudarlo a elegir lo que desea modificar.

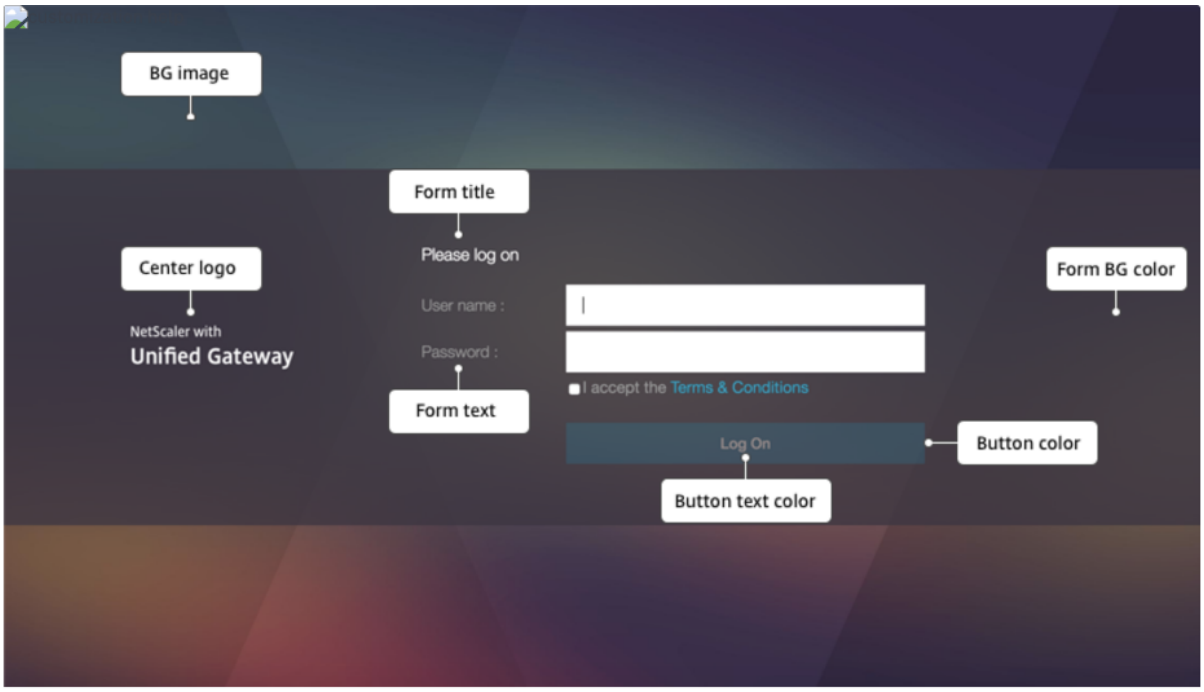


Atributos comunes

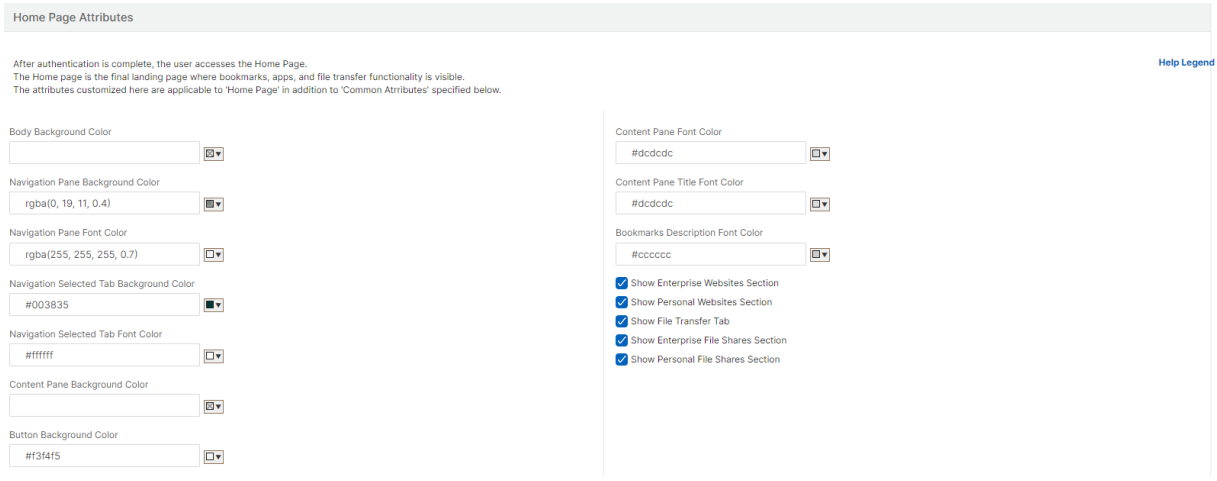
La sección **Atributos comunes** proporciona los parámetros configurables que son comunes a todas las páginas de inicio de sesión de NetScaler Gateway.

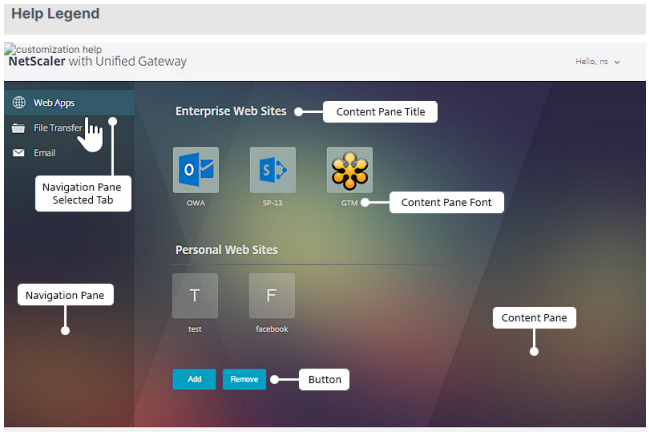


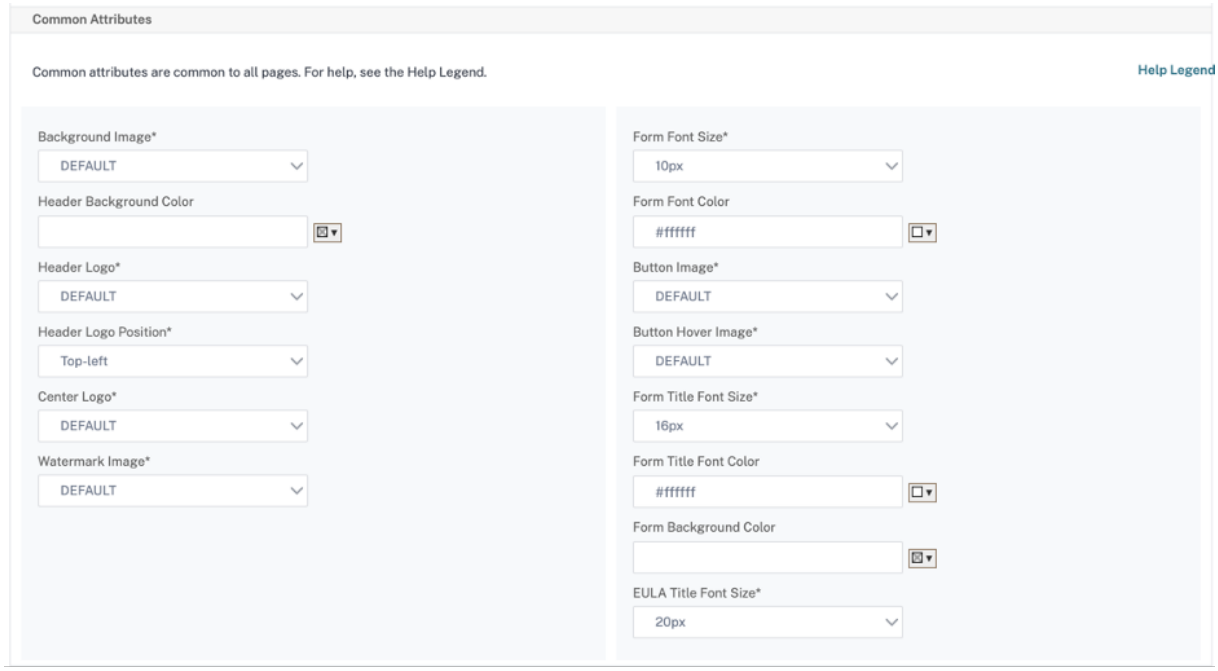
Haga clic en el enlace **Leyenda de ayuda** para ver cada parámetro configurable común.



Del mismo modo, para el tema personalizado basado en **Default**, la siguiente ilustración muestra la configuración disponible para la página principal.
Nota: Esta configuración es diferente para x1 y GreenBubble.





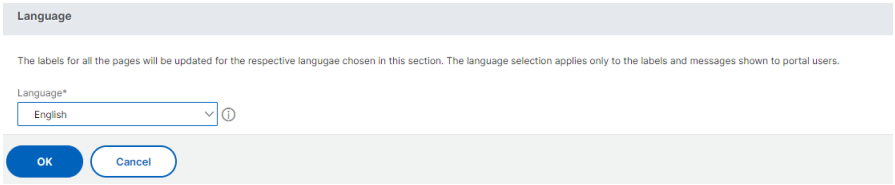


Personalizaciones de cadenas

Además de la apariencia de las páginas de inicio del portal de enlace, la interfaz de usuario de administración también permite la personalización de cadenas en todas las páginas.

Realice los siguientes pasos para personalizar las cadenas:

1. Seleccione el idioma para el que desea modificar la cadena. Las cadenas se muestran en el idioma seleccionado. El inglés está seleccionado de forma predeterminada.



   Nota: El idioma que seleccione no define el idioma del tema del portal. Es el idioma para el que se personalizan las cadenas.

2. A la derecha, en **Configuración avanzada**, se enumeran las páginas que están disponibles para la personalización de cadenas.

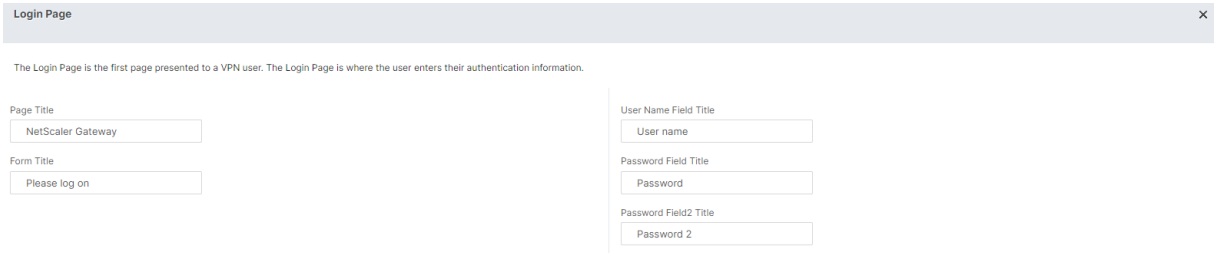
   - Página inicio de sesión
   - Página EPA
   - Página de error EPA
   - Página post-EPA
   - Página Conexión VPN
   - Página de inicio

3. Seleccione la página para la que desea personalizar las cadenas y haga clic en el icono de edición. Se muestra un formulario con personalizaciones de cadenas rellenadas previamente.
4. Seleccione el campo y agregue o modifique la cadena según sus requisitos.
5. Haga clic en **Listo** para completar la creación del tema del portal personalizado. Puede modificar los temas más adelante en **NetScaler Gateway > Temas del portal**.

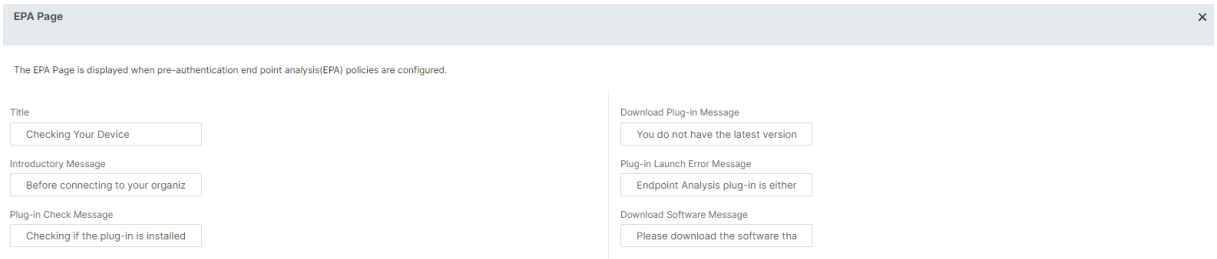
Nota: Si la sección sigue mostrando las cadenas en el idioma seleccionado anteriormente, es posible que la sección ya estuviera abierta cuando se cambió el idioma. En este caso, cierre la sección, seleccione el idioma y vuelva a abrir la página desde **Configuración avanzada**.

Las siguientes capturas de pantalla muestran el conjunto de cadenas personalizables disponibles para cada página.

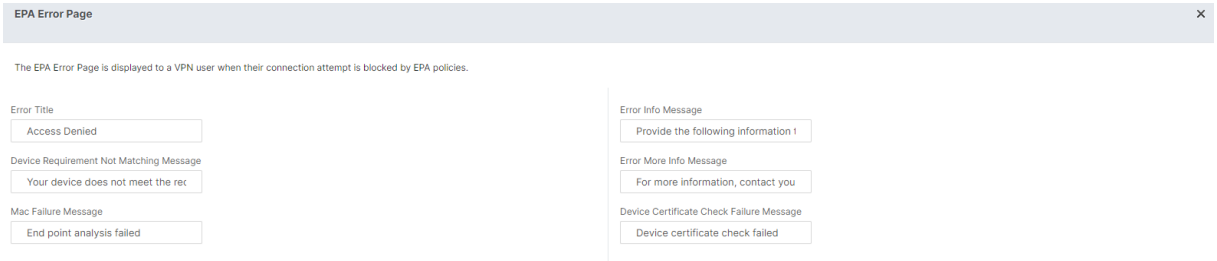
Página inicio de sesión:



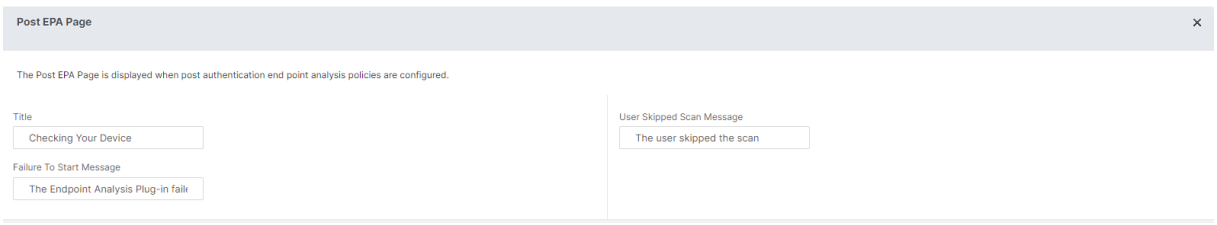
Página EPA:



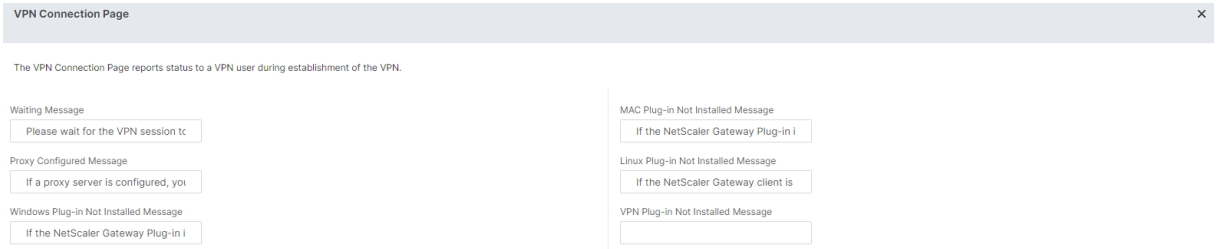
Página Error de la EPA:



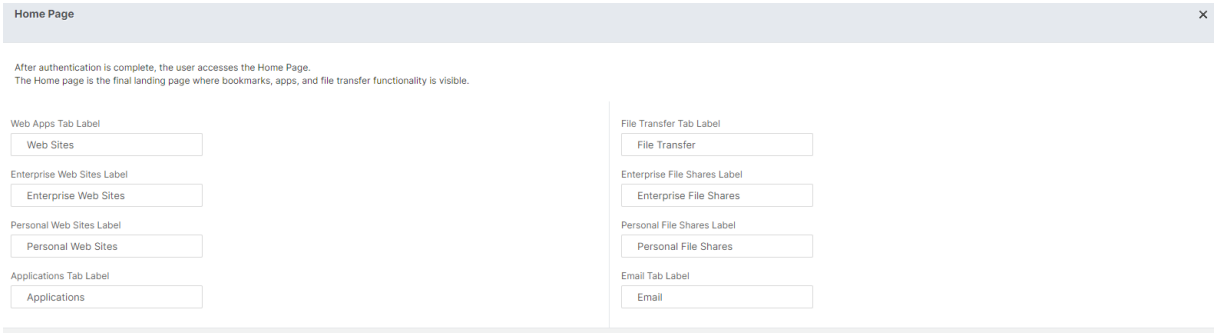
Página posterior a la EPA:



Página Conexión VPN:



Página de inicio:



Optimización del túnel dividido VPN de NetScaler Gateway para Office365

March 27, 2024

Dado que las organizaciones se están adaptando a las opciones de trabajo remoto con mayor rapidez que antes, la infraestructura de acceso remoto debe optimizarse para facilitar una conectividad perfecta durante condiciones de mayor carga de tráfico.

> **Importante:**
>
> Microsoft recomienda excluir el tráfico destinado a los servicios clave de Office 365 del alcance de la conexión VPN mediante la configuración de túneles divididos con los intervalos de direcciones IPv4 e IPv6 publicados. Para obtener el mejor rendimiento y el uso más eficiente de la capacidad de la VPN, el tráfico a los intervalos de direcciones IP dedicadas asociados a las siguientes aplicaciones se debe enrutar directamente, fuera del túnel VPN:
>
> - Office 365 Exchange en línea
> - SharePoint Online
> - Microsoft Teams (denominada categoría Optimizar en la documentación de Microsoft)
>
> Consulte la guía de Microsoft para obtener información más detallada sobre esta recomendación.

La recomendación de Microsoft en NetScaler Gateway se logra mediante la redirección de la lista de direcciones IP proporcionada por Microsoft directamente a Internet para el tráfico de O365 mediante la configuración inversa del túnel dividido.

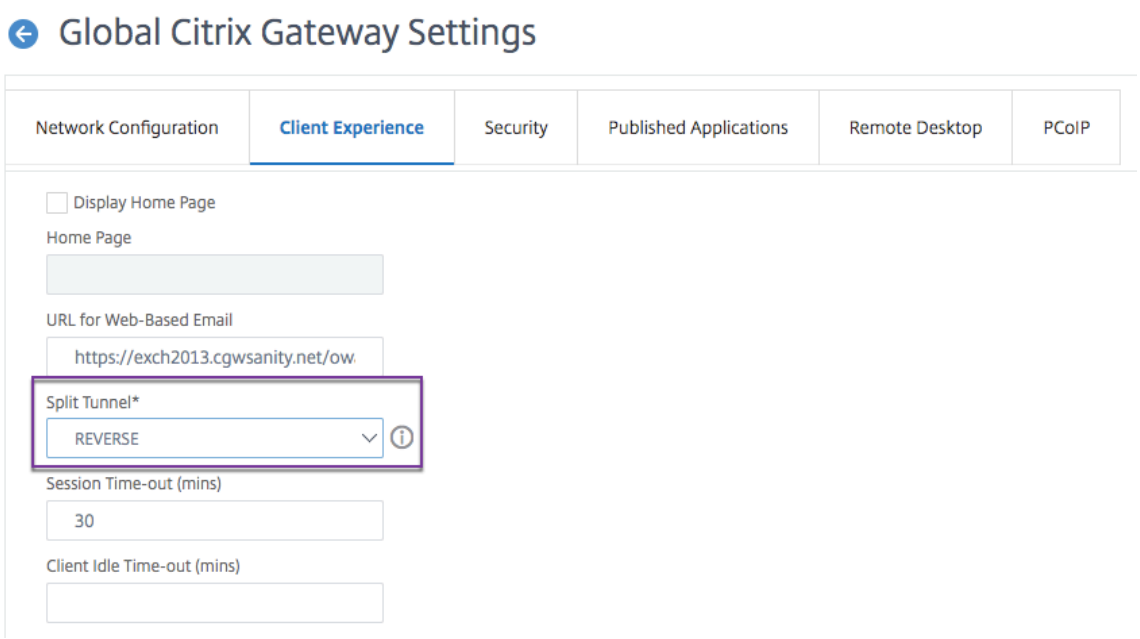
La configuración implica lo siguiente, que se puede realizar manualmente mediante la GUI o la CLI:

- Configure el túnel dividido para la configuración inversa. Para obtener más información, consulte Opciones de tunelización dividida.
- Configure las aplicaciones de intranet para el acceso de los usuarios a los recursos.

Configuración mediante la interfaz gráfica de usuario

Para configurar la tunelización dividida mediante la interfaz gráfica de usuario

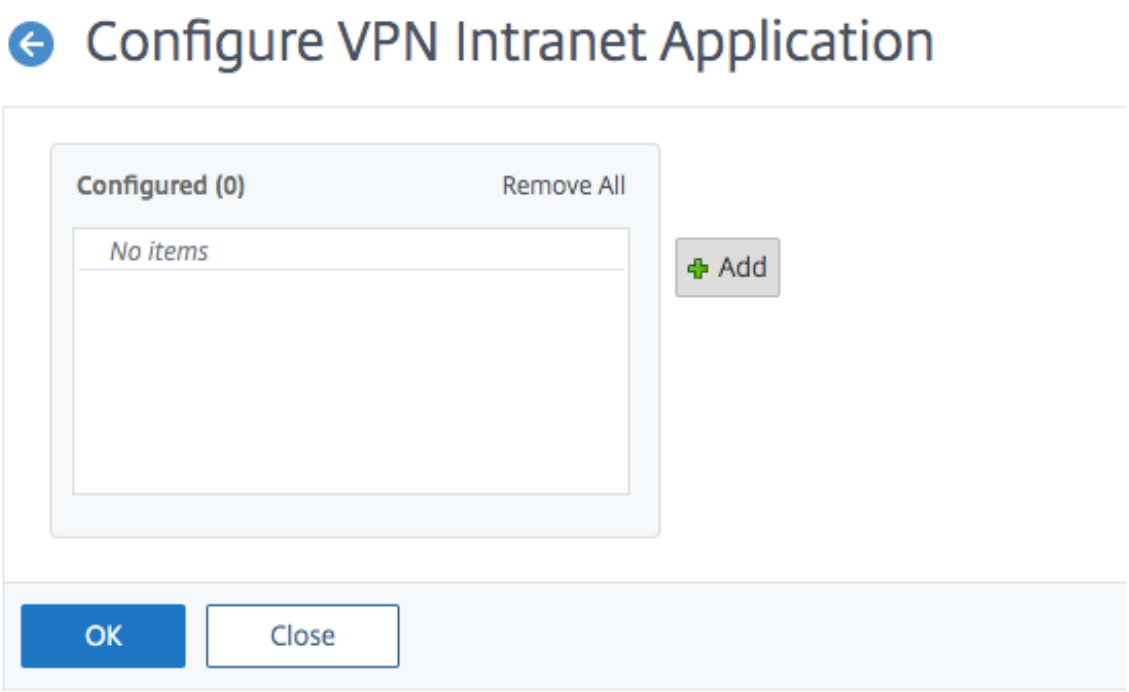
1. En la pestaña Configuración, vaya a **NetScaler Gateway > Configuración global**.
2. En el panel de detalles, en **Configuración**, haga clic en **Cambiar configuración global**.
3. En la ficha **Experiencia del cliente**, en **Túnel dividido**, seleccione **Revertir**.
4. Haga clic en **Aceptar**.

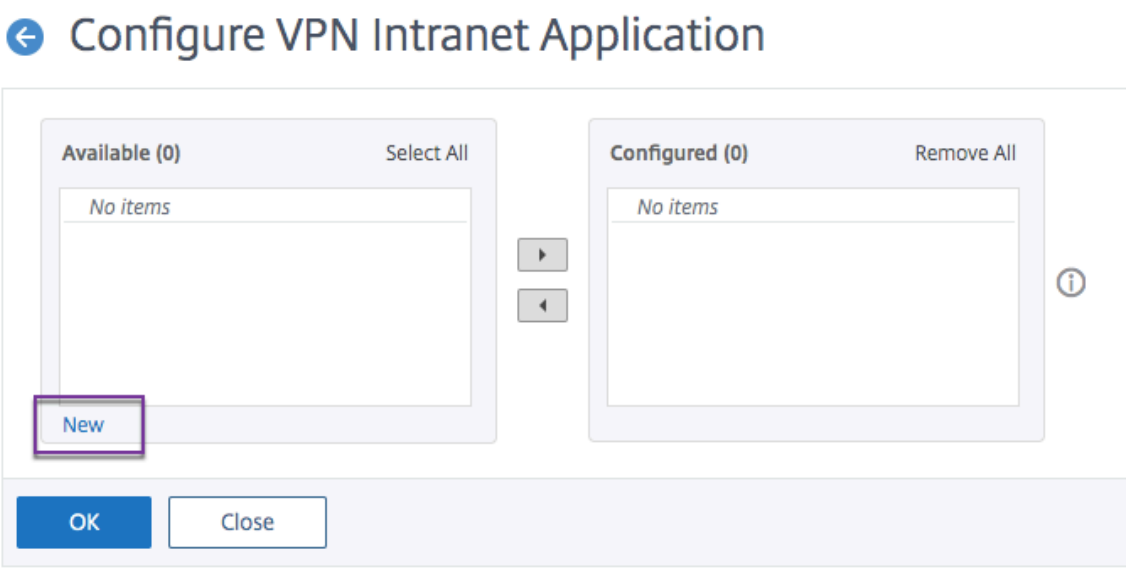


Para crear una aplicación de intranet VPN mediante la interfaz gráfica de usuario

1. En la ficha Configuración, vaya a**Citrix Gateway > Configuración global**.
2. En el panel de detalles, en **Aplicaciones de intranet**, haga clic en el enlace.

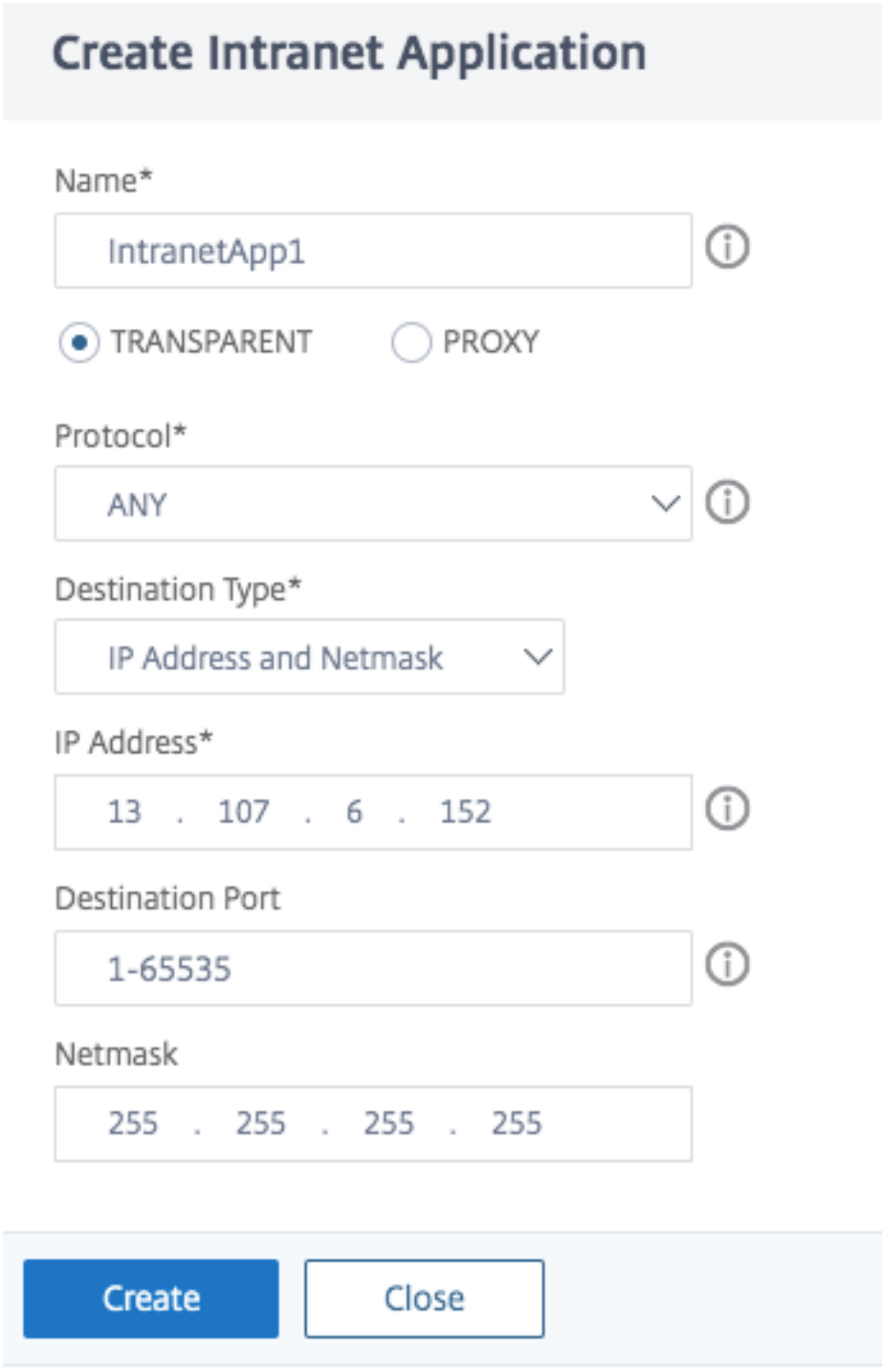
3. En la página **Configurar aplicación de intranet VPN**, haga clic en **Agregar** y, a continuación, en **Nueva**.





4. En **Nombre**, escriba un nombre para el perfil.
5. En **Protocolo**, seleccione el protocolo que se aplica al recurso de red.
6. En **Tipo de destino**, seleccione **Dirección IP y máscara de red**.
7. En **Dirección IP**, introduzca la dirección IP que debe redirigirse directamente a Internet para el tráfico de O365. Para obtener la lista de direcciones IP, consulte Lista de direcciones IP.

8. En **Máscara de red**, introduzca la dirección IP de la máscara de red.



9. Haga clic en **Create** y, luego, en **Close**.

Nota: Repita este procedimiento para todas las direcciones IP.

Configuración mediante la CLI

- Para configurar el túnel dividido para que se invierta, en el símbolo del sistema, escriba;

```
set vpn parameter -splitTunnel REVERSE
<!--NeedCopy-->
```

- Para agregar una aplicación de intranet VPN, en el símbolo del sistema, escriba;

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
   255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
<!--NeedCopy-->
```

Nota: Repita este procedimiento para todas las direcciones IP.

- Para enlazar la aplicación de intranet, en el símbolo del sistema, escriba;

```
bind vpn global -intranetApplication intranetapp1
<!--NeedCopy-->
```

Lista de direcciones IP de los servicios de Office 365 (EXO, SPO y Microsoft Teams)

Referencia: https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

> **Nota de Microsoft:**
>
> Como parte de la respuesta de Microsoft a la situación de la COVID-19, Microsoft ha declarado una moratoria temporal sobre algunos cambios planificados de URL y direcciones IP. Esta moratoria tiene por objeto proporcionar a los equipos de TI de los clientes confianza y simplicidad a la hora de implementar las optimizaciones de red recomendadas para los casos de Office 365 de trabajo desde casa. Desde el 24 de marzo de 2020 hasta el 30 de junio de 2020, esta moratoria detendrá los cambios de los servicios clave de Office 365 (Exchange Online, SharePoint Online y Microsoft Teams) en los rangos de IP y las URL incluidas en la categoría Optimize.

Intervalo de direcciones IPv4

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32

132.245.0.0/16
150.171.32.0/22
150.171.40.0/22
191.234.140.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

Intervalo de direcciones IPv6

2603:1006: :/40
2603:1016: :/36
2603:1026: :/36 2603:1036: :/36
2603:1046: :/36
2603:1096: :/38 2603:1096:400: :/40
2603:1096:600: :/40 2603:1096:a00: :/39
2603:1096:c00: :/40 2603:10 a 6:200: :/40
2603:10 a 6:400: :/40 2603:10 a
6:600: :/40 2603:10 a 6:800: :/40 2603:10 d 6:200: :/40 2620:1 ec:152/128 2620:1 ec:4: :153/128 2620:1 ec:10/128 2620:1 ec:c:
1:11/

128
26201 ec:10/128 2620:1 ec:11/128 262:01 ec:8f0: :/46
2620:1 ec:900: :/46 2620:1 ec:8f8: :/46
2620:1 ec:92:153/128 2a 01:111:f400: :/48 262:01 ec:8f8: :/46
2620:01 ec:908: :/46 2a 01:11:f402:
:/48

Tipo de compatibilidad de servicio para el tráfico UDP

January 26, 2024

La compatibilidad con tipos de servicio (ToS) para UDP garantiza que una vez que un remitente configura un valor ToS para un paquete UDP, NetScaler Gateway conserva el valor hasta que el paquete llegue a su destino. Según el valor configurado y la configuración de la red de destino, la red de destino coloca el paquete UDP en una cola de salida priorizada.

> **Nota:**
> Con la información de ToS, puede asignar una prioridad a cada paquete IP y solicitar un tratamiento específico, como alto rendimiento, alta fiabilidad, baja latencia, etc.

Configuración de la extensión de indicación de nombre de servidor

March 27, 2024

Ahora se puede configurar un dispositivo NetScaler Gateway para incluir una extensión de indicación de nombre de servidor (SNI) en el paquete de saludo del cliente SSL enviado al servidor back-end. La extensión SNI ayuda al servidor back-end a identificar el FQDN que se solicita durante el protocolo de enlace SSL y a responder con los certificados respectivos.

> **Nota**
>
> Habilita la compatibilidad con SNI cuando hay varios dominios SSL alojados en el mismo servidor.

Para configurar NetScaler Gateway para que admita SNI mediante GUI:

1. En la GUI de NetScaler, vaya a **Configuración > NetScaler > Configuración global**.
2. Haga clic en el enlace **Cambiar configuración global** y, en el menú **SNI del servidor backend**, seleccione **Habilitado**.

Para configurar NetScaler Gateway para que admita SNI mediante la interfaz de línea de comandos, en el símbolo del sistema, escriba:

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
<!--NeedCopy-->
```

Validar el certificado del servidor durante un protocolo de enlace SSL

January 26, 2024

El dispositivo NetScaler Gateway ahora se puede configurar para validar el certificado de servidor proporcionado por el servidor back-end durante un enlace SSL.

Para configurar los parámetros globales de NetScaler Gateway para admitir PAC para proxy saliente mediante la utilidad de configuración

Enlazar el certificado de CA

1. Vaya a **Configuración** > **NetScaler Gateway** > **NetScaler Gateway Policy Manager** > **Vinculaciones de certificados**.**
2. En la pantalla **Vinculaciones de certificados**, haga clic en el icono **+**.
3. En la pantalla **Enlace de certificados de CA**, haga clic en **Agregar enlace** y haga clic en **Instalar**.
4. Seleccione el nombre del archivo del certificado en el campo **Nombre del archivo del certificado** y haga clic en **Instalar**.
5. En la pantalla **Enlace de certificados de CA**, seleccione el certificado y haga clic en **Vincular**.
6. Haga clic en **Listo**.

Habilitación de la validación de certificados:

1. Vaya a **NetScaler Gateway > Configuración global.**
2. Haga clic en **Cambiar configuración global**.**
3. Seleccione **Habilitado** en el menú desplegable **Validación de certificados del servidor back-end** y haga clic en **Aceptar**.

Para configurar los parámetros globales de NetScaler Gateway para admitir certificados de servidor con la línea de comandos

En el símbolo del sistema, escriba los comandos siguientes:

```
1     bind vpn global cacert DNPGCA1
2
3     set vpn parameter backendcertValidation ENABLED
4 <!--NeedCopy-->
```

Configuración simplificada de aplicaciones SaaS mediante una plantilla

January 26, 2024

La configuración de aplicaciones SaaS con inicio de sesión único en NetScaler Gateway se simplifica mediante el aprovisionamiento de un menú desplegable de plantillas para aplicaciones SaaS populares. La aplicación SaaS que se va a configurar se puede seleccionar en el menú. La plantilla rellena previamente gran parte de la información necesaria para configurar las aplicaciones. Sin embargo, se debe proporcionar la información específica del cliente.

> **Nota:**
>
> Para configurar y publicar aplicaciones SaaS, configure y publique en NetScaler Gateway y, a continuación, en el servidor de aplicaciones.
>
> Los pasos de la siguiente sección le ayudan a configurar y publicar aplicaciones en NetScaler Gateway mediante una plantilla. A continuación, vaya a la sección que explica cómo configurar y publicar en el servidor de aplicaciones.

Configuración y publicación de aplicaciones mediante plantilla: configuración específica de NetScaler Gateway

En la siguiente configuración se utiliza la aplicación AWS Console como ejemplo de cómo configurar y publicar una aplicación mediante una plantilla.

Antes de empezar, necesitas lo siguiente:

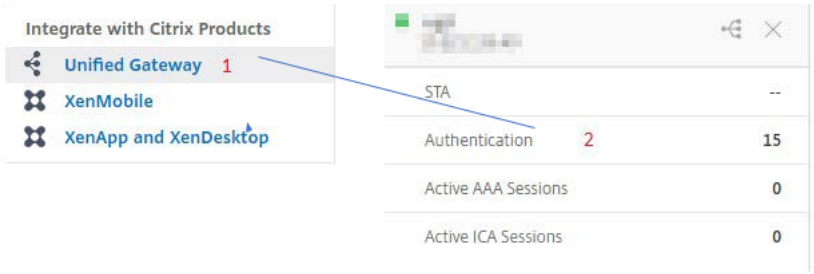
- Una cuenta de administrador para la consola de AWS
- Una cuenta de administrador para NetScaler Gateway

Los pasos de configuración de la consola de AWS son los siguientes:

1. Configure la consola de AWS con el catálogo de aplicaciones.
2. Exportar metadatos de IdP de AWS Console desde NetScaler.
3. Configure el IdP en la consola de AWS.

PASO 1: Configurar la consola de AWS con App Catalog

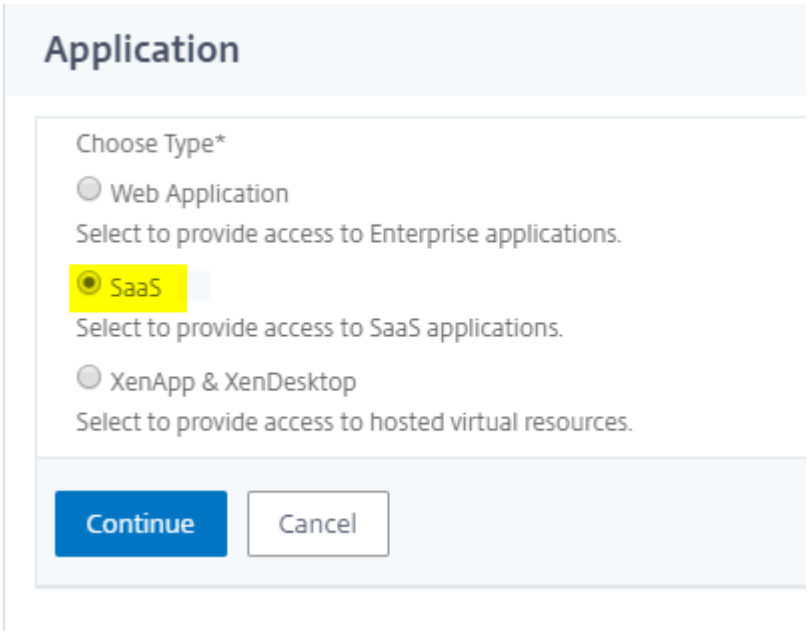
1. Haga clic en **Unified Gateway > autenticación**



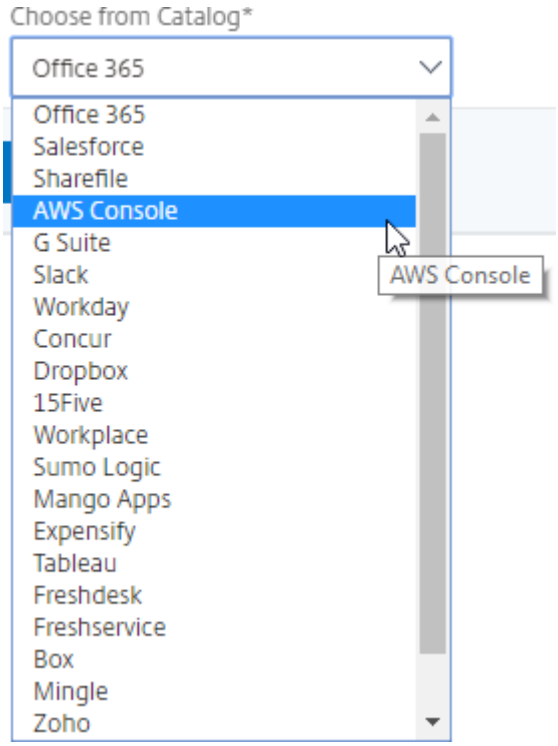
   Aparece la pantalla Configuración de Unified Gateway.

2. En la sección **Aplicaciones**, haga clic en el icono de modificación. Ahora, haga clic en el icono del signo más. Aparece la ventana Aplicación.

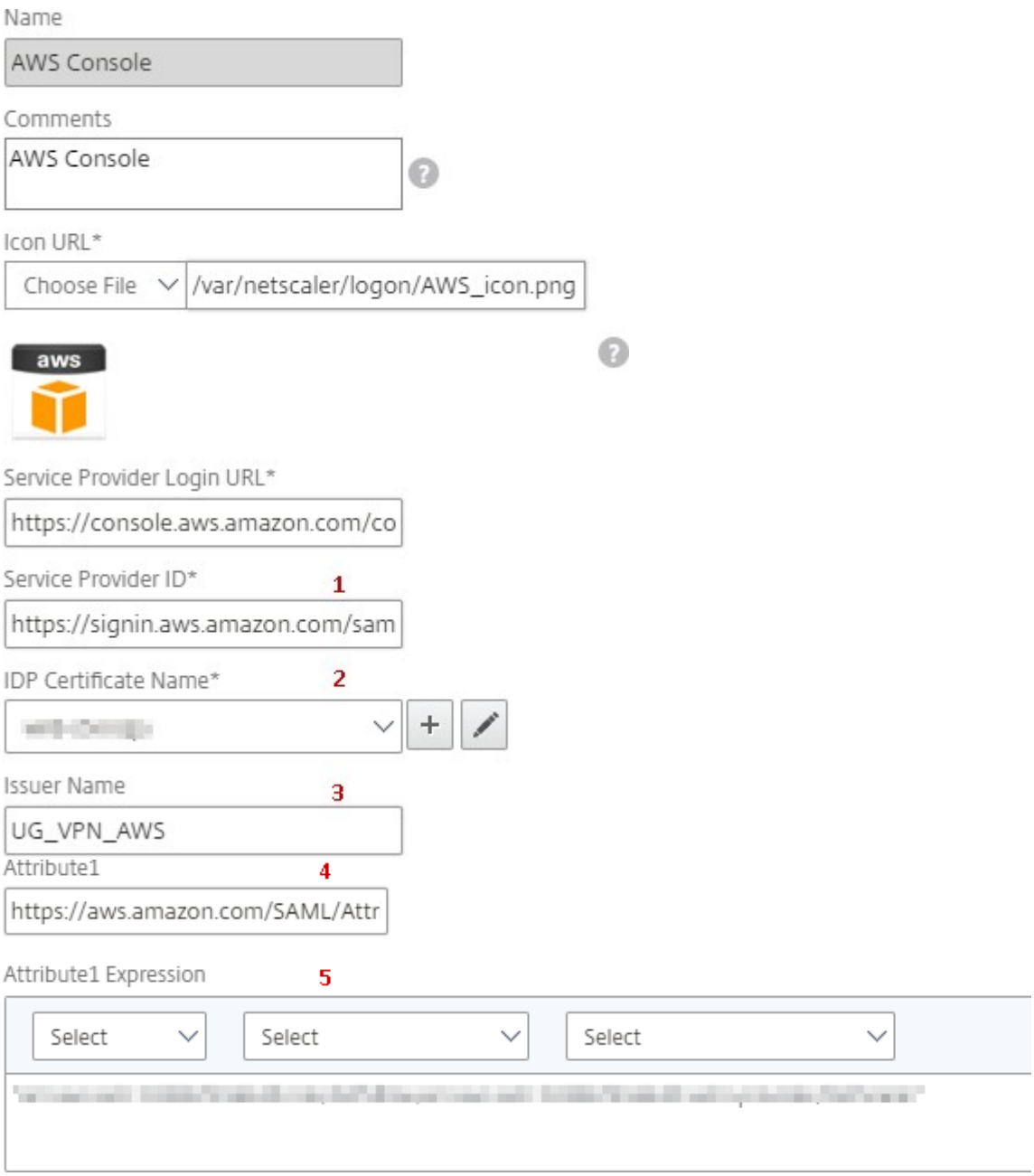
3. Seleccione **SaaS** en el tipo de aplicación.



4. Seleccione **AWS Console** de la lista desplegable.



5. Rellene la plantilla de aplicación con los valores adecuados.



6. Introduzca los siguientes detalles de configuración de SAML y haga clic en **Continuar**.

   ID de proveedor de servicios —https://signin.aws.amazon.com/saml

   Nombre del certificado de firma: Se debe seleccionar el certificado del IdP

   Nombre del emisor: El nombre del emisor se puede rellenar según su elección

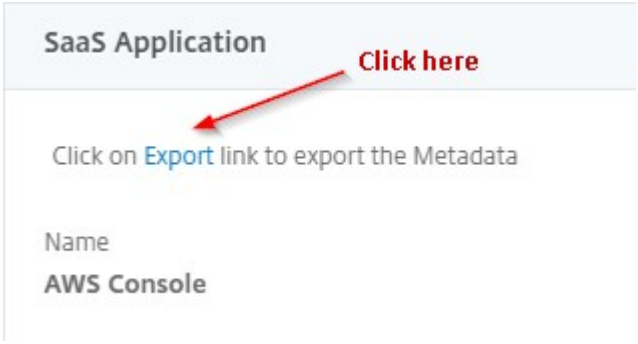
   Atributo 1 —`https://aws.amazon.com/SAML/Attributes/Role`

   Expresión Attribute1 – `Role ARN, IdP ARN`, como se muestra en el paso 3

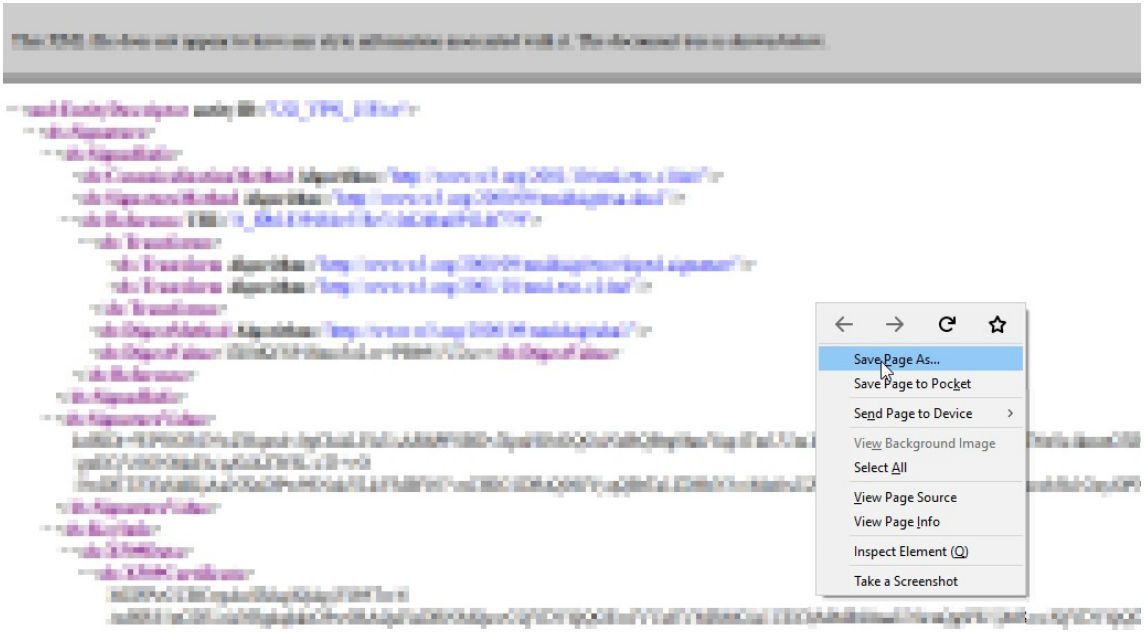
7. Haga clic en **Listo**.

PASO 2: Exporte los metadatos del IdP de la consola de AWS desde NetScaler Gateway.

1. Haga clic en **Unified Gateway > autenticación**
2. Desplácese hacia abajo y haga clic en la plantilla **Consola de AWS**. Aparece la ventana Aplicación SaaS. Haga clic en **Exportar** enlace



3. **Los metadatos** se abrirá en otra ventana. Guardar el archivo de **metadatos del IdP**



PASO 3: Configure el IdP en la consola de AWS.

Configuración y publicación de aplicaciones mediante plantilla: configuración específica del servidor de aplicaciones

En los siguientes enlaces se abren documentos PDF que proporcionan instrucciones específicas para configurar y publicar aplicaciones SaaS populares mediante plantillas.

- 15Five
- Absorb

- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla

- Convo
- Circonus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo
- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub
- GlassFrog

- GotoMeeting
- HappyFox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript
- Marketo

- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard
- Remedyforce

- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria
- Testable

- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret Server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck
- Zendesk

- ZIVVER
- Zoho One
- ZIVVER
- Zoom